

EDPB Strategy 2024-2027



April 2024

The mission and legal task of the **European Data Protection Board (EDPB)** is to ensure the consistent application of EU data protection rules and to promote effective cooperation among data protection authorities throughout the European Economic Area (EEA).

Since their entries into application in 2018, the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) have strengthened, modernised and harmonised data protection across the European Economic Area (EEA). Awareness of data protection rights has risen significantly among data subjects, while controllers and processors in both the public and private sectors have become increasingly aware of their obligations. Meanwhile, supervisory authorities (SAs) are actively using their investigative and corrective powers to effectively enforce the law when appropriate and have reinforced their cooperation. The EDPB has also provided, and will continue to provide, legal and technical guidance on data protection matters. In addition to this guidance, the EDPB has adopted other documents, including binding decisions, to ensure the consistent application of EU data protection laws. The EDPB is committed to continuing all of these works.

The focus of the EDPB has continued to evolve in recent years. In particular, the EDPB has increased its focus on enhancing cooperation among SAs, with the goal of ensuring efficient and consistent enforcement of data protection rules. In the coming years, the EDPB will strengthen this activity while, at the same time, continuing to raise awareness among the wider public, including SMEs, and supporting compliance with the law.

New EU laws which will affect data protection and individuals' data protection rights have been, or will be, introduced in the context of digitalisation. The EDPB reiterates the need for a strong protection of personal data in the context of these laws, including those relating to Artificial Intelligence, the European Data Strategy and the Digital Services Package. We will therefore continue our existing work on the interplay between those laws and the GDPR, while also promoting the necessary supervision of data protection issues, the keeping of individuals at the centre and the effective protection of individuals' rights.

This is also true for the LED, as well as for both the existing and new EU information systems facilitating border control and law enforcement in the broader sense. The EDPB remains committed to ensuring the coordinated supervision of these systems and remains vigilant about the effect that they have on the protection of personal data.

The EDPB will also continue to address the challenges raised by new technologies, such as Artificial Intelligence. It will further engage on these issues to promote high legal standards and cooperation amongst data protection and privacy authorities, and other regulators globally. In light of these objectives, the EDPB's Strategy for 2024 – 2027 is based on four main pillars highlighting our main objectives and the key actions for achieving them. This strategy will be complemented by two Work Programmes and the EDPB will report on the progress achieved as part of our annual report.

Enhancing harmonisation and promoting compliance



Following the EDPB's existing guidance on the key concepts of EU data protection law, we will further enhance our efforts to achieve a consistent application and effective enforcement of the law. One way in which we will do this is by further providing concise and clear guidance on important topics. The EDPB will also develop tools for a wider audience and produce content that is accessible to non-experts, SMEs and other relevant groups (e.g. children). We will also continue to assess how personal data is being accessed and used by public authorities for law-enforcement purposes.

KEY ACTION 1

We will continue providing guidance on key issues. This will include, for example, guidance on the application of the GDPR to particularly vulnerable data subjects, such as children, and on the application of particularly notable provisions, such as legitimate interest. The EDPB reiterates its goal that such guidance will be practical, including the use of examples when appropriate, and be drafted in a way that is accessible to the relevant audience and helps stakeholders to properly implement data protection law.

KEY ACTION 2

We will continue supporting the development and implementation of appropriate and effective compliance measures, such as certification and codes of conduct. As part of this, the EDPB will engage with key groups of stakeholders to, for example, help explain how these tools can be used.

KEY ACTION 3

We will develop information streams which complement our technical and legally-focused publications. These information streams will focus on accessibility and will be tailored for, among others, non-experts, individuals (including children), and SMEs. These may include, for example, information sheets or factsheets which communicate a Guideline's core messages in an accessible way, or further improvements and promotion of the Data Protection Guide for Small Businesses. We will also invest in the visibility of the EDPB and in generating greater awareness about what the EDPB is and does.

PILLAR 2

Reinforcing a common enforcement culture and effective cooperation



Building on the Vienna Statement on enforcement cooperation¹, the “wish list” letter to the EU Commission on procedural aspects that could be harmonised at EU level², and the EDPB-EDPS Joint Opinion 01/2023 on the Proposal laying down additional procedural rules relating to the enforcement of the GDPR³, as well as other EDPB initiatives and actions in this field, the EDPB will further strengthen the efforts to ensure effective enforcement by, and cooperation between, the members of the EDPB. The EDPB will continue to support the development of cooperation and enforcement tools, and the sharing of expertise to increase the robustness of our common procedures, methodologies and decisions.

KEY ACTION 1

We will continue to follow through on the commitments made in the Vienna Statement on enforcement cooperation. In particular, the EDPB will continue to foster the identification of strategic cases for which cooperation will be prioritised and to provide methodologies and tools promoting a harmonised approach to investigation and enforcement. The Support Pool of Experts, the Coordinated Enforcement Framework and the EDPB secondment programme will also be further developed.

KEY ACTION 2

We will reiterate our commitment to the smooth functioning of the One Stop Shop and other cooperation and consistency provisions set out under the GDPR. As part of this, the EDPB will continue to ensure that any requests for Opinions or Binding Decisions under the GDPR consistency mechanisms are fulfilled efficiently by providing clear and robust responses. We also reiterate our commitment to the collegiate nature of the EDPB, including to our task under Article 70(1)(u) GDPR to promote the cooperation and effective bilateral and multilateral exchanges of information and best practices.

KEY ACTION 3

The EDPB will support efforts for the adoption of the EU Regulation laying down additional procedural rules relating to the enforcement of the GDPR, including by continuing to provide feedback on and suggestions for that proposal during the legislative process, as appropriate. Further, we will prepare for its practical implementation. These preparations will include, among other things, a proactive examination of our working methods and procedures to ensure the full application of the opportunities provided by this Regulation.

1. [Statement on enforcement cooperation](#), adopted on 28 April 2022

2. [Letter to Commissioner Reynders](#), sent on 10 October 2022

3. [EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation \(EU\) 2016/679](#), adopted on 19 September 2023

Safeguarding data protection in the developing digital and cross-regulatory landscape



Following developments in the EU regulation of the digital landscape and the rapid developments in technology, the EDPB recognises the need to directly address the role and importance of data protection in the cross-regulatory and interdisciplinary context. As part of our responses to this need, we will promote consistency and cooperation with other regulatory authorities in these contexts, including on topics relating to the regulation of Artificial Intelligence, the European Data Strategy and the Digital Services Package. We will also continue to promote a human-centric approach to new technologies.

KEY ACTION 1

We will provide guidance on the interplay between the application of the GDPR and other EU legal acts, particularly the EU Artificial Intelligence Act or those derived from the EU Data Strategy and the Digital Services Package. This will be done with a view to promoting the right to data protection in the overall regulatory architecture and contributing to a consistent application of different regulatory frameworks. The EDPB will also be ready to apply the consistency mechanism and to adopt binding decisions in the context of the Data Act when personal data is concerned.

KEY ACTION 2

We will continue to monitor and assess new digital technologies to promote a human-centric approach, including those relating to, among others, Artificial Intelligence and digital identity. We will continue to issue guidance, where necessary, on the data protection implications of new technologies, and the correct application of the GDPR in the fast-developing digital landscape. This guidance will, among other things, include a further focus on the implementation of data protection concepts and principles in the context of new technologies, in particular in areas with significant risks for data subjects or where the data subjects belong to a particularly vulnerable group, such as children.

KEY ACTION 3

We will secure cooperation with other regulatory authorities on matters with an impact on data protection, in particular with consumer protection authorities, competition authorities, and authorities competent under other legal acts, including the EU Artificial Intelligence Act or those adopted under the European Data Strategy and the Digital Services Package. Further, the EDPB will continue to take an active role in the DMA High Level Group and the European Data Innovation Board.

PILLAR 4

Contributing to the global dialogue on data protection



The EDPB and its members will continue to promote a global dialogue on privacy and data protection, endorsing the effective protection of data subjects' rights and recognising that data does not stop at the EU border. This includes a focus on the international community and supporting cooperation on enforcement amongst EU and non-EU authorities.

KEY ACTION 1

Building on the EDPB's existing work, we will support the exchange of information and cooperation among EEA data protection authorities active in international forums. We will also continue to engage with the international community, promoting high data protection standards and reinforcing the EDPB's involvement in international discussions. We will, in particular, participate in the global dialogue on data transfers, access to personal data by public authorities and emerging technologies.

KEY ACTION 2

The EDPB will further facilitate and strengthen cooperation between the members of the EDPB and non-EU countries' data protection and privacy authorities. In this context, we will increase our efforts relating to our contributions on international cooperation and supporting enforcement, and further develop our current approaches.

KEY ACTION 3

We will continue working on the GDPR and the LED data transfer mechanisms, including their commonalities with, impact on, and role in the global dialogue. We will continue to focus on specific GDPR tools, including the EDPB's roles in the adequacy decision, certification, code of conduct and binding corporate rule procedures, and we will provide further guidance on the practical implementation of those tools.

Personal data breaches what to do



When processing personal data, an organisation must implement appropriate technical and organisational measures to ensure an adequate level of security.

Despite this, breaches can still occur, so it is important to know how to respond.

The 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".

A data breach can lead to **physical, material, or non material damage** for individuals. This can include loss of control over personal data, limitation of rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, reputation damage, and loss of confidentiality of personal data protected by professional secrecy.

You must document all data breaches in a record, known as **data breach register or documentation**, by adding information about the facts relating to the personal data breach, its effects and the remedial action taken. In the event of an inspection, this documentation can be checked by the competent Data Protection Authority (DPA) to verify compliance with the GDPR.

Many personal data breaches must also be **notified to the DPA and, in certain cases, they must be notified to the individuals** whose personal data have been affected. As a personal data breach is not necessarily an infringement of the GDPR, DPAs are not obliged to exercise their corrective powers.

In case you have fallen victim of cybercrime, you are advised to report it to law enforcement. Europol lists the [reporting procedures in EU countries](#).

The [EDPB guidelines on personal data breach notification under GDPR](#):

- explain when an organisation should report a breach
- provide examples of different types of breaches
- specify who needs to be notified.

These guidelines are complemented by [the guidelines on examples regarding personal data breach notification](#) that provide additional examples to help organisations decide how to manage breaches and assess the risks involved.

There are three kinds of personal data breaches:



Confidential breach

Unauthorised or accidental **disclosure** of, or **access** to, personal data.



Integrity breach

Unauthorised or accidental **alteration** of personal data.



Availability breach

Accidental or unauthorised **loss of access** to, or **destruction** of personal data.



It is always better **to prevent data breaches and reduce the risks by adopting several measures** such as training employees on data protection, using up-to-date anti-virus and anti-malware, keeping systems up to date, implementing access control policies and regularly reviewing employees' access policy, requiring multi-factor authentication for sensitive data access, monitoring unusual data flows, enforcing disk encryption, making and testing backups regularly, and setting computers to auto-lock after inactivity.



A step-by-step approach

1

Identify the breach

Organisations should have **internal processes in place to be able to detect and address a breach**, for instance by analysing appropriate logs or network traffic. When a breach is detected, it should be **reported upwards to the appropriate level of management** so it can be addressed and, if required, notified.

If you rely on processors (who process data under your instructions), they have an important role to help you comply with your obligations, for instance by assisting you in identifying and assessing the breach. You must have a proper agreement in place with them such as a contract or a legal act. It must stipulate, in particular, that processors should assist you in ensuring compliance with your obligations related to personal data breach notification. In the event of a breach, they have an obligation to notify you in a prompt way.

Organisations should **act on any initial alert and establish whether a breach has occurred**.

2

Document the breach

All personal data breaches must be documented in a **register**.

3 Notify the breach to the Data Protection Authority (DPA)

When an organisation is of the opinion that a breach **it is likely to result in a risk to the rights and freedoms of the individual**, it should **notify the relevant DPA no later than 72 hours** after having become aware of the breach. If only limited information is available, an initial notification should be performed within this timeframe, and complemented later, as the breach is being investigated. Notifications sent to the DPA after more than 72 hours must be accompanied by reasons for the delay.

The information that should be shared with the DPA includes:

- the **nature of the personal data breach**
- the **name and contact details of the data protection officer** or of another **contact point** where more information can be obtained
- the **possible consequences of the personal data breach**
- the **measures taken or proposed to be taken to address the breach**.

To facilitate this notification, DPAs have implemented **procedures and online forms** guiding you through this process. If the breach involves cross-border processing, it should be notified to the lead DPA or, at a minimum, the local DPA where the breach has taken place. At the same time, the organisation should act to contain and recover from the breach.

EXAMPLE 1



Context and purpose of processing

An organisation stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.

How to respond

As long as the data are encrypted with a state of the art algorithm, backups of the data exist, the decryption key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, **if it is later compromised, notification would be required**. In any case, **personal data breaches need to be documented**.

EXAMPLE 2



Context and purpose of processing

An insurance agent noticed that, due to faulty settings of an Excel file received by e-mail, he was able to access information related to two dozen customers not belonging to his scope. He is bound by professional secrecy and was the sole recipient of the e-mail. Following the conditions of the arrangement between the organisation and the insurance agent, the agent signalled the breach without undue delay to the organisation. The latter corrected the file and sent it out again, asking the agent to delete the former message and to confirm the deletion in a written statement, which he did.

How to respond

This data breach only affects the confidentiality of the data, while its integrity and accessibility remain unaffected. The data breach affected only about two dozen customers, which can be considered a relatively small number of individuals. Furthermore, the personal data affected does not contain any sensitive data.

The fact that the data processor immediately contacted the data controller after becoming aware of the data breach can be considered a risk mitigating factor. Due to the appropriate steps taken after the data breach, it will probably not have any impact on the individuals' rights and freedoms.

Therefore, **this case should not be notified to the Data Protection Authority and individuals. Data breach documentation remains a legal obligation.**

4 Notify the breach to affected individuals

Where the breach is **likely to result in a high risk to the rights and freedoms of individuals**, affected individuals must also be informed as soon as possible in order to be able to protect themselves from any negative consequences of the breach.

In some cases, and based on law enforcement authorities' advice, the organisation may delay informing affected individuals about the breach if it could interfere with an investigation. However, individuals should still be notified as soon as possible after that delay.

To inform individuals about a data breach, organisations should send dedicated messages via appropriate channels such as e-mails, SMS, direct messages, website banners or notifications. Communication channels compromised by the breach should be avoided. If needed, the communication should be done in different languages.

EXAMPLE 3



Context and purpose of processing

A hospital's information system was hit by a ransomware attack, encrypting much of its data. The hospital is working with an external cybersecurity firm to monitor its network. Logs of all data leaving the hospital, including outbound email, were reviewed. The investigation, supported by the cybersecurity firm, confirmed that the attacker only encrypted the data, not exfiltrated it.

How to respond

The type of the breach, nature, sensitivity, and volume of personal data affected in the breach are important. Even though a backup for the data existed and it could be restored in a few days, a high risk still exists as the breach led to major delays in treating the patients with surgery cancelled / postponed, and to a lowering of the level of service due to the unavailability of the systems.

In this case, **the data breach should be notified both to the Data Protection Authority and the affected individuals. Data breach documentation is also a legal obligation.**

EXAMPLE 4



Context and purpose of processing

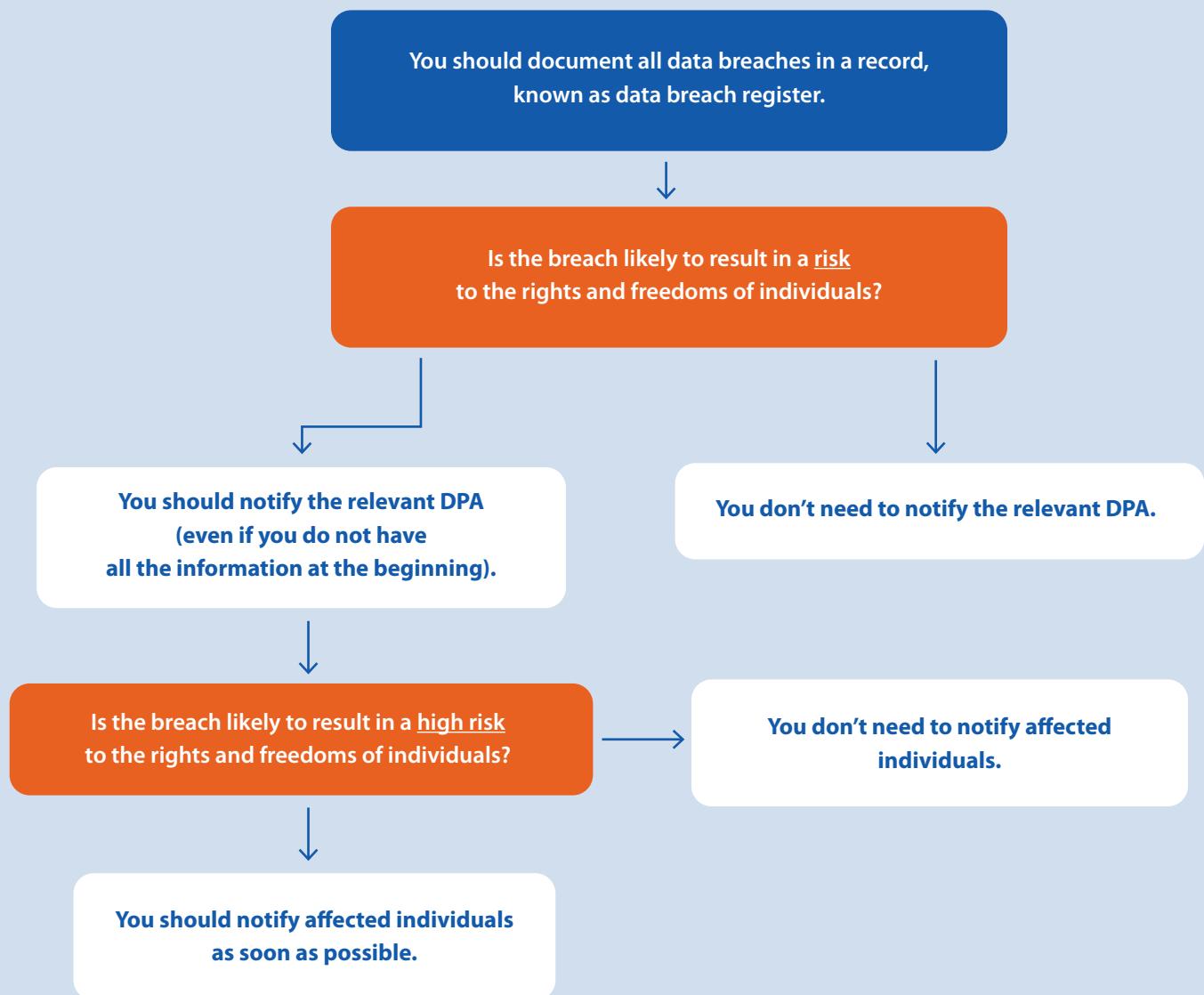
A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals were exfiltrated.

How to respond

A notification to the supervisory authority is needed if there are likely consequences to individuals. Notification to individuals depends on the nature of the personal data affected and if the severity of the consequences to individuals is high.

Data breach documentation is also a legal obligation.

In a nutshell:



If you rely on processors (who process data under your instructions), they have an important role to help you comply with your obligations, for instance by assisting you in identifying and assessing the breach.

[Read more](#)

 [Guidelines 9/2022](#)

 [Guidelines 01/2021](#)

Binding decision of the Board (Art. 66)



**Urgent Binding Decision 01/2021 on the request under
Article 66(2) GDPR from the Hamburg (German) Supervisory
Authority for ordering the adoption of final measures
regarding Facebook Ireland Limited**

Adopted on 12 July 2021

Table of contents

1	Summary of the facts	4
2	Competence of the EDPB to adopt an urgent binding decision under Article 66(2) GDPR	7
2.1	Existence of a request pursuant to Article 66(2) GDPR coming from a SA in the EEA.....	7
2.2	The SA has taken provisional measures under Article 66(1) GDPR.....	7
2.3	Conclusion	7
3	The Right to good administration.....	7
4	On the need to request final measures.....	8
4.1	On the existence of infringements	8
4.1.1	Summary of the overall position of the DE-HH SA	8
4.1.2	Security and integrity of Facebook.....	10
4.1.3	Improvement of product experience	18
4.1.4	Marketing communications and direct marketing.....	29
4.1.5	WhatsApp Business API.....	32
4.1.6	Cooperation with other Facebook Companies.....	38
4.1.7	Conclusion	41
4.2	On the existence of urgency to adopt final measures by way of derogation from the cooperation and consistency mechanisms	41
4.2.1	Possible application of a legal presumption of urgency justifying the need to derogate from the cooperation and consistency mechanisms	42
4.2.2	Existence of urgency outside any GDPR legal presumption and the need to derogate from the cooperation and consistency mechanisms	43
4.2.3	Conclusion	47
5	On the appropriate final measures	47
6	Urgent Binding Decision	48
7	Final remarks	49

The European Data Protection Board

Having regard to Article 66 of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter “**GDPR**”)¹,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018²,

Having regard to Articles 11, 13, 23 and 39 of the EDPB Rules of Procedure³, hereinafter the “**EDPB RoP**”.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**” or the “**Board**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it can adopt binding opinion and decisions under different circumstances described under the Articles 63 to 66 GDPR. The GDPR also established a cooperation mechanism between the supervisory authorities. It follows from Article 60 GDPR that the lead supervisory authority shall cooperate with the other supervisory authorities concerned (hereinafter “**CSAs**”) in an endeavour to reach consensus.

(2) Pursuant to Article 66(1) GDPR, in exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 GDPR or the procedure referred to in Article 60 GDPR, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months.

(3) In accordance with Article 66(2) GDPR, where a supervisory authority has taken a measure pursuant to Article 66(1) GDPR and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision. The request for an urgent opinion or urgent binding decision in the context of Article 66(2) and (3) GDPR is optional.

(4) In accordance with Article 11(2) EDPB RoP, the request of a binding decision shall be submitted to the EDPB via the information and communication system mentioned in Article 17 EDPB RoP.

(5) In accordance with Article 13(2) EDPB RoP, the supervisory authority requesting an urgent binding decision shall submit any relevant documents. When necessary, the documents submitted by the competent supervisory authority shall be translated into English by the EDPB Secretariat. Once the Chair and the competent supervisory authority have decided that the file is complete, it is communicated via the EDPB Secretariat to the members of the Board without undue delay.

(6) Pursuant to Article 66(4) GDPR and Article 13(1) EDPB RoP, the urgent binding decision of the EDPB shall be adopted by simple majority of the members of the EDPB within two weeks following the decision by the Chair and the competent supervisory authority that the file is complete.

¹ OJ L 119, 4.5.2016, p. 1.

² References to “Member States” made throughout this decision should be understood as references to “EEA Member States”. References to “EU” should be understood, where relevant, as references to “EEA”.

³ EDPB Rules of Procedure, adopted on 25 May 2018, as last modified and adopted on 8 October 2020.

(7) Pursuant to Article 39(1) EDPB RoP, all the final documents adopted by the Board shall be made public on the Board's website, unless the Board decides otherwise.

1 SUMMARY OF THE FACTS

1. This document contains an urgent binding decision adopted by the EDPB pursuant to Article 66(2) GDPR, following a request made by the Hamburg Commissioner for Data protection and freedom of information (hereinafter the “**DE-HH SA**”) within the framework of the urgency procedure under Article 66 GDPR.
2. Following the notification by WhatsApp Ireland Ltd (hereinafter “**WhatsApp IE**”) to German users of its new Terms of Service and Privacy Policy, and the extension of the deadline for users to provide consent to 15 May 2021, the DE-HH SA came to the conclusion that Facebook Ireland Ltd (hereinafter “**Facebook IE**”) is already processing data of WhatsApp users residing in Germany for its own purposes in some cases, and that processing for its own purposes is imminent in other cases. The DE-HH SA considers that the processing of personal data of WhatsApp IE users residing in Germany by Facebook IE for the purposes of Facebook IE violates Article 5(1), Article 6(1) and Article 12(1) GDPR. Therefore the DE-HH SA adopted, on 10 May 2021, provisional measures under Article 66(1) GDPR, based on its consideration that the circumstances were exceptional and there was an urgent need to act to protect the rights and freedoms of data subjects.
3. Through its provisional measures, the DE-HH SA prohibited, for a duration of 3 months, Facebook IE from processing personal data of WhatsApp users residing in Germany, which is transmitted from WhatsApp IE to Facebook IE for the purposes of 1. Cooperation with other Facebook Companies⁴; 2. Security and integrity of Facebook; 3. Improvement of the product experience; 4. Marketing communication and direct marketing; 5. WhatsApp Business API; to the extent that the processing is being carried out for Facebook IE's own purposes.
4. On 7 June 2021, the DE-HH SA requested the EDPB to adopt an urgent binding decision pursuant to Article 66(2) GDPR, with the effect of ordering the implementation of final measures, by extending its provisional measures both in time and territorial scope.
5. The following table presents a summarised timeline of the events leading to the submission of the matter by the DE-HH SA via the urgency procedure:

08.12.2020	The Irish supervisory authority (“Data Protection Commission”, hereinafter the “ IE SA ” or, as being the lead supervisory authority in this case, the “ LSA ”) uses the EDPB internal information and communication system (the “ IMI system ”) flow “Voluntary Mutual Assistance” (hereinafter “ VMA ”) to inform the CSAs that WhatsApp IE intends to change its Privacy Policy and Terms of Service applicable to users residing in the European Union (hereinafter “ Updated Terms ”). The LSA shares copies of the revised Privacy Policy, including a redline version highlighting the changes (hereinafter the “ Privacy Policy ”), the Legal Basis Notice (which will be incorporated in the Privacy Policy), the relevant extract from the Terms of Service, the contact upload feature and the updated
------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

⁴ A link inserted in WhatsApp public-facing information sends to a page on WhatsApp explaining that the term ‘**Facebook Companies**’ refers to Facebook Inc., Facebook IE, Facebook Payments Inc., Facebook Payments International Limited, Facebook Technologies LLC, Facebook Technologies Ireland Limited, WhatsApp LLC, and WhatsApp IE. In this urgent binding decision, the term ‘**other Facebook Companies**’ refers to all the Facebook Companies except WhatsApp IE.

	version of the FAQ “How we work with the Facebook Companies” (hereinafter together referred to as “WhatsApp public-facing information”).
14.01.2021	The DE-HH SA sends a letter to the LSA using the IMI system flow opened by the LSA. It raises the fact that the LSA did not provide its view on the Updated Terms, and shares questions on the Updated Terms, including questions directly addressed to the LSA.
15.01.2021	The IE SA sends a letter to the CSAs to inform them that it met with WhatsApp IE to discuss the new Updated Terms, that the IE SA will compile comprehensive feedback from the CSAs, and will transmit it to WhatsApp IE for follow-up. Few days after, the LSA shares with the CSAs, via VMA, a letter from WhatsApp IE dated 5 February 2021 replying to questions raised by the CSAs, including the DE-HH SA.
12.02.2021	The DE-HH SA shares a letter with the LSA using the same VMA flow on the IMI system. The DE-HH SA underlines the fact that the LSA did not share its own views on the matter. The DE-HH SA informs the LSA about its concerns regarding the data sharing of Facebook IE and WhatsApp IE for different purposes of each company. The DE-HH SA concludes that <i>“WhatsApp and Facebook are sharing data for different purposes of each company. In the case of no deeper inspection by the IDPC as lead authority we give notice of the possibility of an urgency procedure according to Art. 66 GDPR.”</i>
24.02.2021	Using VMA, the LSA replies to the DE-HH SA by sharing the fact that it had forwarded the additional questions on Updated Terms to WhatsApp IE on 15 February 2021. The LSA also annexes to its message to DE-HH SA WhatsApp IE’s latest reply dated 22 February 2021.
04.03.2021	Using VMA, the DE-HH SA sends a new letter to the LSA in which it underlines the substantial need for further clarifications and makes comments on the Updated Terms and the answers provided by WhatsApp IE. The DE-HH SA requests the LSA to conduct investigations into the specific processing of WhatsApp IE and Facebook.
12.04.2021	The DE-HH SA contacts Facebook IE to hear it before issuing provisional measures pursuant to Article 66 (1) GDPR. The DE-HH SA informs the EDPB Secretariat that they intend to start a formal Article 66 GDPR procedure against Facebook IE, and asks the EDPB Secretariat to inform the Chair of the EDPB and the LSA. Following a later request from the DE-HH SA, the EDPB Secretariat also shares the information with all the EDPB members.
19.04.2021	Using VMA, the LSA writes to the CSAs to inform them that the Updated Terms are <i>“[...] largely a carryover of the text of the existing policy and no new text signifying any change in WhatsApp’s position is included regarding the sharing of WhatsApp user data with Facebook or access by Facebook for Facebook’s own purposes”</i> . The IE SA informs the CSAs that it commenced a supervision review and assessment of WhatsApp IE’s oversight and monitoring of its data processors (chiefly Facebook), including the safeguards, mechanisms and audit processes in place to ensure that Facebook IE does not use WhatsApp IE user data for its own purposes, inadvertently or otherwise.
25.04.2021	Facebook IE sends written submissions following the hearing letter of the DE-HH SA (hereinafter “Facebook’s written submissions to the DE-HH SA”).
10.05.2021	The DE-HH SA adopts an order relating to provisional measures (the “DE-HH SA Order” or the “provisional measures”).
11.05.2021	The DE-HH SA communicates its provisional measures to the other supervisory authorities and informs the EDPB Secretariat.

03.06.2021	The DE-HH SA writes to the EDPB Chair to announce the request of an urgent binding decision under Article 66(2) GDPR.
04.06.2021	Via VMA, the IE SA informs the CSAs that, contrary to WhatsApp IE's previous intention to limit functionality for its users who had not accepted the Updated Terms after several weeks following the deadline it had set to 15 May 2021, WhatsApp IE announced in an updated published FAQ that it has no plans for these reminders to become persistent and to limit the functionality of its app.
07.06.2021	The DE-HH SA introduces the request of an urgent binding decision under Article 66(2) GDPR in the IMI system (Article 17 EDPB RoP). On 25 June 2021, the DE-HH SA reintroduced the file in IMI for technical reasons.

6. On 7 June 2021, the DE-HH SA requested an urgent binding decision under Article 66(2) GDPR via IMI, the information and communication system mentioned in Article 17 EDPB RoP.
7. On 9 June 2021, the EDPB Secretariat, working on behalf of the Chair of the EDPB, requested via email an additional document to the DE-HH SA, as well as confirmation of the accuracy of the English translation of documents received in German, with the deadline of 11 June 2021. Following a request sent by the DE-HH SA on 10 June 2021 to extend the deadline to 16 June 2021, the EDPB Secretariat extended the deadline up to 14 June 2021. On 14 June 2021, the DE-HH SA sent the additional document and approved the English translation of the original German documents.
8. On 15 June 2021, the EDPB sent a letter to Facebook IE and to WhatsApp IE thereby allowing Facebook IE and WhatsApp IE to exercise their respective right to be heard with the deadline of 18 June 2021. This letter included a list of all the documents in the file and attached them all, except the ones originating from Facebook IE or WhatsApp IE. On 16 June 2021, Facebook IE asked an extension of deadline to 23 June 2021 close of business. The EDPB replied on the same day and consented to extend the deadline to 23 June 2021 12:00 (CET).
9. On 18 June 2021, the EDPB Secretariat, working on behalf of the Chair of the EDPB, urgently requested additional documents from the DE-HH SA, which were provided on the same day. On 21 June 2021, the EDPB sent a letter to Facebook IE and to WhatsApp IE with the additional documents provided by the DE-HH SA, and taking into account of these new elements, extended the deadline for both companies to provide their written contribution to 25 June 2021 12:00 (CET).
10. On 23 June 2021, the IE SA sent, on its own initiative, additional documents it considered important to be added in the file. The Chair of the EDPB agreed and decided to add two documents in the file. On 24 June 2021, the Chair informed WhatsApp IE and Facebook IE about those two additional documents, and extended the deadline for their written submission to 25 June 2021 16:00 (CET).
11. On 25 June 2021, Facebook IE and WhatsApp IE provided their written submissions to the EDPB.
12. On 28 June 2021, after the DE-HH SA and the Chair of the EDPB confirmed the completeness of the file, the EDPB Secretariat circulated the file to the EDPB members.
13. On 5 July 2021 12:00 (CET), the EDPB decided, in accordance with Article 11 EDPB RoP, to add in the file the redline version of the FAQ "How we work with the Facebook Companies" highlighting the changes made at the occasion of the Updated Terms, which was shared by the IE SA. On the same day, the EDPB sent a letter to Facebook IE and WhatsApp IE to invite them to provide additional written

submissions about a legal argument discussed between the EDPB members and the redline version of the FAQ “How we work with the Facebook Companies”, with a deadline of 6 July 2021 12:00 (CET). Following Facebook IE and WhatsApp IE’s request, the deadline was extended to 7 July 16:00 (CET). On 7 July 2021, Facebook IE and WhatsApp IE provided their written submissions to the EDPB.

2 COMPETENCE OF THE EDPB TO ADOPT AN URGENT BINDING DECISION UNDER ARTICLE 66(2) GDPR

2.1 Existence of a request pursuant to Article 66(2) GDPR coming from a SA in the EEA

14. Following the adoption of provisional measures under Article 66(1) GDPR on 10 May 2021, the DE-HH SA requested the EDPB to adopt an urgent binding decision pursuant to Article 66(2) GDPR, by introducing a formal request in the IMI (Article 17 EDPB RoP) on 7 June 2021.
15. The EDPB therefore considers that this condition is fulfilled.

2.2 The SA has taken provisional measures under Article 66(1) GDPR

16. On 10 May 2021, the DE-HH SA adopted provisional measures pursuant to Article 66(1) GDPR, prohibiting Facebook IE from processing the personal data of WhatsApp users residing in Germany, which are transmitted from WhatsApp IE or WhatsApp LLC to Facebook IE for the purposes of (1) cooperation with other Facebook Companies; (2) security and integrity of Facebook; (3) improvement of the product experience; (4) marketing communication and direct marketing; (5) WhatsApp Business API; to the extent that the processing is being carried out for Facebook IE's own purposes.
17. The EDPB therefore considers that this condition is fulfilled.

2.3 Conclusion

18. The EDPB is competent to adopt an urgent binding decision under Article 66(2) GDPR.

3 THE RIGHT TO GOOD ADMINISTRATION

19. The EDPB is subject to the EU Charter of fundamental rights (hereinafter the “**EU Charter**”), in particular its Article 41 (right to good administration). This is also reflected in Article 11(1) EDPB RoP.
20. Similarly, as provided under Article 65(2) GDPR, an Article 66(4) EDPB urgent binding decision is addressed to the national supervisory authorities and binding on them. It is not aimed to address directly any third party. However, as a precautionary measure, and in order to address the possibility that Facebook IE and WhatsApp IE might be affected by the EDPB urgent binding decision, the EDPB assessed whether all the documents it received and used in order to take its decision were already known by Facebook IE and WhatsApp IE, and whether Facebook IE and WhatsApp IE had been heard on them.
21. While Facebook IE was heard during the DE-HH SA’s national procedure, on the basis of Article 66(1), neither Facebook IE nor WhatsApp IE had been heard yet on the DE-HH SA’s Article 66(2) GDPR

request. The EDPB therefore decided to hear directly Facebook IE and WhatsApp IE by inviting them to provide written submissions to the EDPB.

22. During the assessment of the completeness of the file, the EDPB shared all the documents of the file (see above the para 9, 10, 11 and 14) to Facebook IE and WhatsApp IE directly to ensure the exercise of their right to be heard in line with Article 41(2)(a) EU Charter.
23. Facebook IE and WhatsApp IE provided written submissions to the EDPB in the context of their right to be heard on 25 June 2021, 6 July 2021, and 7 July 2021 (respectively hereinafter “**Facebook’s written submissions to the EDPB**” and “**WhatsApp’s written submissions to the EDPB**”).

4 ON THE NEED TO REQUEST FINAL MEASURES

4.1 On the existence of infringements

4.1.1 Summary of the overall position of the DE-HH SA

24. According to the DE-HH SA, Facebook IE is already processing data of WhatsApp users for its own purposes or will imminently do so.
25. The DE-HH SA’s analysis is based on WhatsApp’s public-facing information such as Terms of Service and privacy-related public-facing information, including WhatsApp’s Privacy Policy applicable to EU users and FAQ, as well as Facebook IE’s written submissions in the context of its hearing carried out by the DE-HH SA before adopting the provisional measures, including, *inter alia*, an affidavit signed by Facebook IE’s Head of Data Protection on 25 April 2021 (hereinafter the “**Affidavit**”)⁵, which adheres and supports commitments WhatsApp IE took towards the Article 29 Working Party (hereinafter the “**WP29**”) and the LSA (hereinafter the “**Commitments**”)⁶, respectively in February and June 2018.
26. The DE-HH SA considers that Facebook IE has no legal basis for the processing of WhatsApp user data for its own purposes, hence it is unlawful due to the lack of effective consent of WhatsApp users within the meaning of Article 6(1)(a) and Article 7 GDPR, and of a legitimate interest within the meaning of Article 6(1)(f) GDPR.
27. The DE-HH SA considers that the consent requested by WhatsApp in its Terms of Service of 4 January 2021 does not meet the requirements of informed and free consent within the meaning of Article 6(1)(a) and Article 7 GDPR⁷.
28. The DE-HH SA states that the Updated Terms are not understandable by users; they do not comply with the transparency requirements under Article 5(1)(a), Article 12(1) and Article 13(1)(c) and (e)) GDPR; the explanations on data exchange are partly contradictory and inconsistent, as well as largely undefined⁸; the statements on data exchange are scattered in various documents at different levels⁹

⁵ Facebook’s submissions to the DE-HH SA. This also includes (Letter from WhatsApp IE to the WP29 dated 4 February 2018, p.1; and Letter from WhatsApp IE to the IE SA dated 8 June 2018, p. 2).

⁶ Facebook’s submissions to the DE-HH SA. This also includes (Letter from WhatsApp IE to the WP29 dated 4 February 2018, p.1; and Letter from WhatsApp IE to the IE SA dated 8 June 2018, p. 2).

⁷ DE-HH SA Order, Section II.2)aa), p. 13.

⁸ DE-HH SA Order, p. 14.

⁹ There are in total 15 documents linked to the terms, with a total of 20.000 words (DE-HH SA Order, pp. 5-6).

and do not allow users to take note of them in a uniform manner¹⁰. The DE-HH SA also explains why the transparency requirements are not fulfilled in relation to each of the specific purposes it identified (see hereinafter)¹¹.

29. In addition, the DE-HH SA underlines that considering the market position of Facebook and WhatsApp, users do not have a choice to **consent** or not, as not using WhatsApp is not an acceptable alternative because of the wide use of such a closed messenger system¹². According to the DE-HH SA, it is not possible to continue the use of WhatsApp's service on the basis of WhatsApp's previously applicable terms and conditions.
30. The DE-HH SA states that Article 6(1)(b) GDPR is not relevant as the transfer of WhatsApp user data to by Facebook IE, and further processing by the latter for its own purpose, is not necessary for the **performance of a contract** concluded between WhatsApp IE and the data subjects¹³ or between Facebook IE and the data subjects¹⁴. For those WhatsApp users who are not Facebook users, the DE-HH SA considers that there is already a lack of corresponding contractual relationship between Facebook IE and such concerned WhatsApp users.
31. The DE-HH SA notes that, should Facebook IE use Article 6(1)(f) GDPR as a ground for such processing , it would need to transparently inform users about this on the basis of Article 13(1)(c) GDPR. Moreover, according to the DE-HH SA, even for purposes for which a **legitimate interest** may exist, for example to prevent the sending of spam in the area of network security, Facebook's legitimate interest does not outweigh the fundamental rights and freedoms of the users. The DE-HH SA underlines in particular the large amount of data processed, which cannot be justified by Facebook's legitimate interests¹⁵. The DE-HH SA also raises that there is a complete lack of necessity for the data sharing with Facebook IE of WhatsApp users that are not Facebook users¹⁶.
32. Besides, the DE-HH SA underlined a violation of the transparency requirements under Article 5(1) GDPR and Article 12(1) GDPR¹⁷. This is due to the large number of different documents that users need to read to understand what is done with their personal data; to the inadequate consideration of the fact that users usually access such information via their smartphones, which, from a technical perspective, makes it more difficult to comprehend; to the existence of two versions of Terms of Service (one for users within the EEA and one for users from the rest of the world); and to how easy it is for users in the EEA to confuse the public-facing information applicable to them and the information applicable to non-EEA users¹⁸.
33. The DE-HH SA identified five processing purposes which it considers are already being carried out or could be carried out imminently by Facebook IE as a controller: 1) Security and integrity of Facebook; 2) Improvement of the product experience; 3) Marketing communication and direct marketing; 4)

¹⁰ DE-HH SA Order, Section II.2)aa), p. 14. 2 versions of the Terms of Service exist, one for the EEA and one for the rest of the world, and EEA users may access pages for non EEA users without even noticing it, DE-HH SA Order, p. 7.

¹¹ DE-HH SA Order, Section II.2)aa), p. 15-28.

¹² Letter of the DE-HH SA requesting an EDPB urgent binding decision, p. 4.

¹³ DE-HH SA Order, Section II.2)aa), p. 2.

¹⁴ DE-HH SA Order, Section II.2)aa), p. 28.

¹⁵ DE-HH SA Order, Section II.2)aa), p. 29-30.

¹⁶ DE-HH SA Order, Section II.2)aa), p. 29-30.

¹⁷ DE-HH SA Order, p. 2.

¹⁸ DE-HH SA Order, p. 3.

WhatsApp Business API; and 5) Cooperation with other Facebook Companies. These purposes are subject to the provisional measures ordered by the DE-HH SA and are further assessed hereinafter.

4.1.2 Security and integrity of Facebook

4.1.2.1 Summary of the position of the DE-HH SA

34. According to the DE-HH SA, the other Facebook Companies process WhatsApp user data for their own security and integrity purposes. They are not acting in the context of a commissioned processing on behalf of WhatsApp IE, but rather carry out an independent processing of WhatsApp user data¹⁹.
35. For the DE-HH SA, the processing aiming at combatting spam and abuse on other Facebook services than WhatsApp; protecting such other Facebook services; and ensuring the security of all Facebook Companies constitutes a separate purpose that is part of Facebook IE's own purposes²⁰.
36. The DE-HH SA notes that there is ambiguity in WhatsApp's FAQ²¹ on the meaning of the term 'our services', which actually refers to all services of Facebook Companies, including WhatsApp's. It could therefore be assumed that the same meaning is used for the other parts of WhatsApp's user-facing information, in which case Facebook IE extensively uses WhatsApp user data as a controller²².
37. The DE-HH SA's views on the Commitments relating to safety and security²³ are the following:
 - | The statements that no sharing of WhatsApp user data is taking place with Facebook, including Facebook IE, for Facebook's own purposes of safety and security only excludes that such sharing is currently taking place, but they do not exclude that Facebook IE is processing WhatsApp user data for its own purposes of safety and security, or that such processing is at least imminent²⁴.
 - | WhatsApp's user-facing information does not reflect the Commitments since it mentions this processing as taking place already²⁵. Besides, such voluntary Commitments are not, by nature, legally binding²⁶, and "*the GDPR does not provide for "consent" or "authorisation" for data*

¹⁹ DE-HH SA Order, Section II.2)aa), p. 17.

²⁰ DE-HH SA Order, Section II.2)aa), p. 19.

²¹ DE-HH SA Order, Section II.2)aa), p. 17, in particular footnote 13, and p. 19.

²² DE-HH SA Order, Section II.2)aa), p. 19.

²³ Facebook IE referred to the Commitments by which WhatsApp IE had not started to share the data of WhatsApp users residing in Germany with Facebook IE for safety and security purposes and on a controller-to-controller basis, and should it change, to do so "*following further engagement and consultation with [the IE SA]*", and that it intends to only share such data on a case-by-case basis, "*for example sharing of data related to individuals previously identified as a safety or security risk*" (Facebook's written submissions to the DE-HH SA, Annex 1, Letter from WhatsApp IE to the WP29 dated 4 February 2018, p. 2, and Letter from WhatsApp IE to the IE SA dated 8 June 2018, p. 2). Facebook IE assured that the Commitments were still accurate as "German WhatsApp users' data" are not shared yet by WhatsApp IE with Facebook Companies, including Facebook IE for Facebook's own safety and security purposes (Facebook's written submissions to the DE-HH SA, Annex 2, the Affidavit, point B., 4th paragraph).

²⁴ DE-HH SA Order, Section III, p. 30.

²⁵ DE-HH SA Order, Section III, p. 31.

²⁶ In Facebook IE's opinion, WhatsApp IE's "*clear and unequivocal*" Commitments to the WP29 and the IE SA fall within the controller's obligation to cooperate with a SA - which has enforcement powers - in accordance with Article 31 GDPR. Facebook IE added that it "*takes compliance with [WhatsApp IE's] Commitments very seriously*" (Facebook's written submissions to the DE-HH SA, section 2.7, p. 9).

processing operations by [SAs]. The formulated restriction is therefore without legal significance.”²⁷

38. Overall, the DE-HH SA concluded that WhatsApp IE shares all its user data with Facebook IE “(...) for the purposes of making the systems more secure and combating spam, threats, abuse and rights violations for all products of the Facebook companies”²⁸.

4.1.2.2 Analysis of the EDPB

39. The EDPB assessed the security and integrity purpose in relation to the alleged unlawful processing of WhatsApp user data by Facebook IE as a controller, and in relation to the alleged infringement of the transparency requirements in WhatsApp’s user-facing information. The EDPB took into account the views of the DE-HH SA, as well as the position expressed by both Facebook IE and WhatsApp IE.

4.1.2.2.1 On the alleged unlawful processing of WhatsApp user data by Facebook IE as a controller

40. In relation to safety, security and integrity, the EDPB notes the following extracts from WhatsApp’s user-facing information (emphasis added underlined):
41. WhatsApp’s Privacy Policy applicable to users living in the European Union:

“Third-Party Information [...]”

Third-Party Service Providers. We work with third-party service providers and other Facebook Companies to help us operate, provide, improve, understand, customise, support, and market our Services. For example, we work with them to [...]; provide engineering support, cybersecurity support, and operational support; [...] ensure safety, security and integrity; and help with customer service. These companies may provide us with information about you in certain circumstances; [...].

The “How We Work With Other Facebook Companies” section below provides more information about how WhatsApp collects and shares information with the other Facebook Companies. You can also learn more in our Help Center on how we work with the Facebook Companies. [...]

Information You And We Share [...]”

Third-Party Service Providers. We work with third-party service providers and other Facebook Companies to help us operate, provide, improve, understand, customise, support, and market our Services. We work with these companies to support our Services, such as to [...] protect the safety, security and integrity of users and others; [...]. When we share information with third-party service providers and other Facebook Companies in this capacity, we require them to use your information on our behalf in accordance with our instructions and terms. For further information on how the Facebook Companies help us to operate and provide our Services, see “How We Work With Other Facebook Companies” below. You can also learn more in our Help Center on how we work with the Facebook Companies. [...]

How We Work With Other Facebook Companies

As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the other Facebook Companies to promote safety, security and integrity across the Facebook Company Products, e.g., to fight spam, threats, abuse, or infringement activities. WhatsApp also works, and shares information with the other Facebook Companies who act on our behalf to help us operate, provide, improve, understand, customise, support, and market our Services. This includes

²⁷ DE-HH SA Order, Section III, p. 31.

²⁸ DE-HH SA Order, Section II.2)aa), p. 20.

the provision of infrastructure, technology, and systems, [...] and securing systems. When we receive services from the Facebook Companies, the information we share with them is used on WhatsApp's behalf and in accordance with our instructions. Any information WhatsApp shares on this basis cannot be used for the Facebook Companies' own purposes. We've set out further information in our Help Center about how WhatsApp works with the Facebook Companies. [...]

How We Process Your Information - Provision Of The Services In Accordance With The Terms
[...] Legitimate Interests

We rely on our legitimate interests or the legitimate interests of a third party where they are not outweighed by your interests or fundamental rights and freedoms ("legitimate interests"):

Why And How We Process Your Data:

- [...] *To share information with the Facebook Companies to promote safety and security and integrity. See also "How We Work with Other Facebook Companies" for more information.*
 - *Legitimate Interests Relied On: To secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products.*
 - *Data Categories Used: We use information described in the "Information You Provide," "Automatically Collected Information," and "Third-Party Information" sections of this Privacy Policy for this purpose."*

42. WhatsApp's FAQ "How we work with the Facebook Companies" (emphasis added underlined):

"Why does WhatsApp share information with the Facebook Companies?

WhatsApp works and shares information with the other Facebook Companies to receive services like infrastructure, technology, and systems that help us provide and improve WhatsApp and to keep WhatsApp and the other Facebook Companies safe and secure. When we receive services from the Facebook Companies, the information we share with them is used to help WhatsApp in accordance with our instructions. Working together allows us for example to:

- [...] Ensure safety, security, and integrity across WhatsApp and the Facebook Company Products by removing spam accounts and combating abusive activity. [...].

What information does WhatsApp share with the Facebook Companies?

[...] WhatsApp also shares information with other Facebook Companies when this is necessary for the purpose of promoting safety, security, and integrity across the Facebook Companies. This includes the sharing of information that enables Facebook and the other Facebook Companies to determine whether a certain WhatsApp user is also using other Facebook Company Products, and to assess whether the other Facebook Companies need to take action, either against such user or to protect them. For example, WhatsApp could share the information that is necessary to enable Facebook to also take action against an identified spammer on Facebook, such as information on the incident(s) as well as the phone number they verified when they signed up for WhatsApp or device identifiers associated with the same device or account. Any such transfer is carried out in accordance with the "Our Legal Basis For Processing Data" section of the Privacy Policy.

How is my WhatsApp information used by the Facebook Companies?

- [...] To keep WhatsApp and other Facebook family services safe and secure.
 - We share information with the other Facebook Companies in accordance with the "Our Legal Basis For Processing Data" section of the Privacy Policy, and vice versa, to help fight spam and abuse on our Services, help keep them secure, and promote safety, security, and integrity on and off our Services. So if, for example, any member of the Facebook Companies discovers that someone is using its services for illegal purposes, it can disable their account and notify

the other Facebook Companies so that they can also consider doing the same. In this way, we only share information for this purpose in relation to users that have first been identified as having violated our having violated our Terms of Service or threatened the safety or security of our users or others, about which other members of our family of companies should be warned.

- To keep WhatsApp and other Facebook Companies' services safe and secure, we need to understand which accounts across the Facebook Companies relate to the same user, so we can take appropriate action when we identify a user who violates our Terms of Services or presents a safety or security threat to others."

43. In their written submissions to the EDPB, Facebook IE and WhatsApp IE referred to the Commitments made to the WP29 and the IE SA, i.e., "[...] following the GDPR Update [in 2018] WhatsApp intended to commence the sharing of its EU users' data with Facebook on a controller-to-controller basis for safety and security purposes only. We made this clear to our users in the User Engagement Flow and our Privacy Policy as well as explaining to users the legal bases on which we will rely for this sharing, which includes legitimate interest, contractual necessity, vital interests and public interest". It also includes the following: "However, it's important to note that WhatsApp has not yet commenced the sharing of this data with Facebook on this basis. Whilst we plan to commence this sharing in the foreseeable future, we can confirm that WhatsApp will only do so following further engagement and consultation with [the IE SA]. For your information, as and when we do commence this sharing (which, as I say, will only follow further engagement and consultation with your Office) our current intention is that it would only involve sharing of data on a case by case basis, for example sharing of data related to individuals previously identified as a safety or security risk."
44. Facebook IE also stated that: "The current status quo is that Facebook companies other than WhatsApp Ireland (collectively "Facebook") process WhatsApp user data shared by WhatsApp Ireland as processors acting on the latter's behalf and under its instructions. Neither Facebook Ireland nor any of the other Facebook companies are conducting any of the Alleged Processing²⁹ – i.e. no Facebook companies, other than WhatsApp Ireland, are processing such WhatsApp user data as controllers (the "Status Quo")"³⁰.
45. This statement was further confirmed in the Affidavit³¹, according to which "It has also been confirmed to me by WhatsApp Ireland that German WhatsApp users' data is not being provided to Facebook Ireland (or any other Facebook Company) by WhatsApp Ireland on a controller-to-controller basis for it to be used for Facebook's own safety and security purposes. It has been confirmed to me by WhatsApp Ireland that this will only occur in the future following further engagement and consultation with the [IE SA] (who in turn I believe, again, would consult with other supervisory authorities concerned as appropriate under Art. 60 GDPR). Again, I can confirm my understanding from my role at Facebook Ireland that Facebook Ireland supports and adheres to the commitments WhatsApp Ireland has made in this regard."

²⁹ Facebook's written submissions to the EDPB dated 25 June 2021, para. 20. In Facebook's written submissions to the EDPB, 'Alleged Processing' is defined by reference to the processing prohibited by the DE-HH SA Order, i.e., "[...] Facebook Ireland [...] processing personal data of WhatsApp users residing in Germany [...] transmitted by WhatsApp Ireland to Facebook Ireland as a controller, for a broadly described list of Facebook Ireland's own purposes", para. 3.

³⁰ Facebook's written submissions to the EDPB dated 25 June 2021, para. 20.

³¹ This Affidavit was first attached to Facebook's written submissions to the DE-HH SA, and provided again in Facebook's written submissions to the EDPB as Annex 2.

46. Facebook IE repeated its support and adherence to the Commitments once more in its written submissions to the EDPB, explaining that “[...] to remove any possibility for concern in this respect, Facebook Ireland has already provided clear confirmation to the [DE-HH SA] that it supports and adheres to the Commitments and hereby expressly confirms such adherence again.”³²
47. In reference to the DE-HH SA’s claim that the Commitments were not legally binding, Facebook IE submitted “[...] that under Article 31 GDPR, WhatsApp Ireland as a controller is legally obligated to cooperate with the [IE SA] as LSA, which has extensive enforcement powers under GDPR as well as Irish law. Therefore, neither WhatsApp Ireland nor Facebook Ireland could simply cease to comply with the Commitments in the manner the [DE-HH SA] alleges. On the contrary, both companies are dedicated to upholding the Commitments [...].”³³
48. Furthermore, Facebook IE submitted that the wording included in WhatsApp’s FAQ “How we work with the Facebook Companies” (see relevant extract above) “[...] does not support in any way the allegations made by the [DE-HH SA]. It is not indicative of the Alleged Processing, other than in respect of the planned future controller-to-controller sharing of WhatsApp User Data for safety and security purposes, which (a) has been provided for in WhatsApp’s privacy policies since at least 2016, and which (b) will only be commenced by WhatsApp Ireland following further engagement with the IDPC, in line with the Commitments. This quote otherwise relates (i) to processing which Facebook conducts as a service provider and processor for WhatsApp Ireland’s purposes, on the latter’s behalf and under its instructions; or (ii) to situations where no EU WhatsApp user data is shared.”³⁴
49. In relation to the quote at stake, the EDPB observes that it expressly sets out that WhatsApp’s user data shared with the other Facebook Companies to receive services from the latter, for example in relation to safety, security and integrity across WhatsApp and the products offered by the other Facebook Companies is done in accordance with WhatsApp IE’s instructions. On Facebook IE’s claim that the extract may concern “situations where no EU WhatsApp user data is shared”, the EDPB notes that such extract is included under the heading “Why does WhatsApp share information with the Facebook Companies?”.
50. According to Facebook IE, the extract from the FAQ “How we work with the Facebook Companies” (see para. 43 above) “is a simplified and accessible explanation of complex technical processing operations, which is designed to assist users of varying sophistication in understanding how their data is being processed by WhatsApp Ireland. It was not intended to provide a detailed explanation of complex legal concepts contained in the GDPR, nor can its wording provide sufficient basis on which to conclude a regulatory process on such matters³⁵”.
51. Based on these statements, the EDPB notes that Facebook IE is unambiguous about the fact that it intends to start processing WhatsApp’s user data as a controller for the purpose of safety, security and integrity of the other Facebook Companies, but is less clear on whether it is currently processing WhatsApp’s user data for that same purpose, as an alleged processor. In its letter addressed to the EDPB on 7 July 2021, Facebook IE stated that this “is not taking place and will not take place premised on the WhatsApp Update”.
52. The EDPB observes that in their current drafting, the statements included in WhatsApp’s user-facing information do not mirror the Commitments by providing an indication to users that this processing

³² Facebook’s written submissions to the EDPB dated 25 June 2021, para. 28.

³³ Facebook’s written submissions to the EDPB dated 25 June 2021, para. 27.

³⁴ Facebook’s written submissions to the EDPB dated 25 June 2021, para. 36.

³⁵ Facebook’s written submissions to the EDPB dated 7 July 2021, p. 5.

for safety, security and integrity purpose is, for now, only a plan, whereas the Commitments relating to product improvement and advertising are mirrored in WhatsApp's user facing information.

53. Transparency obligations stem from Article 5(1)(a) and Article 12(1) GDPR. They are an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 EU Charter³⁶. Hence, controllers' public-facing data protection statements aim at explaining to data subjects how and why their personal data are processed and at empowering them to exercise control over their personal data by exercising their rights enshrined in Chapter III GDPR. To that end, it is of the utmost importance that public facing statements mirror the processing undertaken or to be imminently undertaken by controllers, in order to provide a fairly accurate description of what data subjects may reasonably expect in relation to the processing of their personal data when reading privacy policies and other public-facing statements (e.g., FAQs).
54. Therefore, the EDPB shares the DE-HH SA's position that there are contradictions between the information included in WhatsApp's user-facing information on the one hand, and the Commitments and Facebook IE's written submissions on the other hand.
55. According to the GDPR, a controller is "[...] the natural or legal person, [...] which, alone or jointly with others, determines the purposes and the means of the processing of personal data"³⁷, hence is serving its own interests³⁸.
56. The EDPB remarks that, in the analysis of a processing which may be divided into several smaller processing operations and which involves several actors, it is important to consider whether, at "macro-level", these processing operations should not be considered as a "set of operations" pursuing a joint purpose using jointly defined means³⁹. Besides, the EDPB recalls that the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, therefore the concept of 'controller' should be interpreted in a sufficiently broad way, favouring as much as possible effective and complete protection of data subjects so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules, while at the same time not diminishing the role of the processor⁴⁰.
57. In relation to the determination of means, the EDPB recalls that a distinction can be made between essential and non-essential means, whereby:
 - ✓ Essential means are to be determined by the controller, and are closely linked to the purpose and the scope of the processing (e.g., type of personal data which are processed, duration of the processing, categories of recipients, categories of data subjects).
 - ✓ Non-essential means can be determined by the controller or the processor, and concern more practical aspects of implementation (e.g., choice for a particular type of hard- or software or the detailed security measures)⁴¹.

³⁶ See WP29 Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (WP260 rev.01), endorsed by the EDPB on 25 May 2018, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/transparency_en, para 2.

³⁷ See Article 4(7) GDPR.

³⁸ See by analogy, EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (final version after public consultation adopted on 7 July 2021), para 80.

³⁹ See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version, para. 43.

⁴⁰ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 14.

⁴¹ See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version, para. 40.

58. In relation to the concept of joint controllership, the EDPB considers that it “[...] can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing.”⁴² As per converging decisions, the EDPB specifies that “[a]n important criterion [...] is whether the processing would not be possible without both parties’ participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.”⁴³ Besides, the EDPB observes that “[j]oint controllership exists when entities involved in the same processing carry out the processing for jointly defined purposes. This will be the case if the entities involved process the data for the same, or common, purposes.”⁴⁴
59. According to the GDPR, a processor is ““[...] the natural or legal person, [...] which processes personal data on behalf of the controller”⁴⁵, hence is serving the interests of someone else⁴⁶ and may not carry out processing for its own purpose(s)⁴⁷.
60. The EDPB takes note of Facebook IE’s claim that the other Facebook Companies only process WhatsApp IE’s user data shared by the latter as WhatsApp IE’s processors, and that the processing identified by the DE-HH SA as being allegedly performed by the other Facebook Companies are processing WhatsApp IE’s user data shared by the latter as controllers, is not taking place⁴⁸.
61. The EDPB remarks that it is unclear from WhatsApp’s user-facing information, whether the processing of WhatsApp’s user data by WhatsApp IE and the other Facebook Companies, for the common purpose of safety, security and integrity across WhatsApp and the other Facebook Companies is currently being carried out by Facebook IE as a processor acting under the instructions of WhatsApp IE (see for instance (emphasis added underlined): “When we receive services from the Facebook Companies, the information we share with them is used to help WhatsApp in accordance with our instructions. Working together allows us for example to: • [...] Ensure safety, security, and integrity across WhatsApp and the Facebook Company Products by removing spam accounts and combating abusive activity. [...]”⁴⁹); or being carried by Facebook IE as a (joint) controller with WhatsApp IE (see for instance (emphasis added underlined), “As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the other Facebook Companies to promote safety, security and integrity across the Facebook Company Products, e.g., to fight spam, threats, abuse, or infringement activities, e.g., to fight spam, threats, abuse, or infringement activities.”⁵⁰).
62. Furthermore, whilst the EDPB acknowledges the Commitments, and the Affidavit, the EDPB notices the use of ambiguous wording by both Facebook IE and WhatsApp IE in both documents (e.g., “shared” could exclude covering other processing operations; “by WhatsApp Ireland” could exclude covering sharing by other Facebook Companies; “any of the Alleged Processing” could exclude covering the

⁴² See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version Executive summary.

⁴³ See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version para. 55.

⁴⁴ See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version para. 59.

⁴⁵ See Article 4(8) GDPR.

⁴⁶ See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version para. 80.

⁴⁷ See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version para. 81.

⁴⁸ Facebook’s written submissions to the EDPB dated 25 June and 7 July 2021.

⁴⁹ See the FAQ “How we work with the Facebook Companies”, *Why does WhatsApp share information with the Facebook Companies?*

⁵⁰ See the FAQ “How we work with the Facebook Companies”, *How We Work With Other Facebook Companies*

processing of WhatsApp users residing outside Germany; “such WhatsApp user data” could exclude WhatsApp users residing outside Germany or WhatsApp user data shared by WhatsApp IE).

63. In addition, the EDPB observes that the fact that “*for the purpose of promoting safety, security, and integrity across the Facebook Companies*”⁵¹, WhatsApp’s user-facing information refers to the current exchange of data between WhatsApp IE and the other Facebook Companies “[...] to determine whether a certain WhatsApp user is also using other Facebook Company Products, and to assess whether the other Facebook Companies need to take action, either against such user or to protect them”⁵² and “*To keep WhatsApp and other Facebook Companies’ services safe and secure, we need to understand which accounts across the Facebook Companies relate to the same user*”⁵³, means that, from a practical perspective, WhatsApp’s user data would need to be combined or at least compared with the data of users of products and services offered by the other Facebook Companies. In their response to the EDPB dated 7 July 2021, Facebook IE and WhatsApp IE submitted that the sharing of WhatsApp’s user data with the other Facebook Companies for Facebook IE’s own purpose of safety and security is not taking place, and did not further comment on any possible combination or comparison of WhatsApp’s user data with other data sets controlled by Facebook IE for the purpose of safety, security and integrity.
64. Should it actually take place in practice, WhatsApp and Facebook Companies’ decision to combine or at least compare at individual level the personal data of their respective users - possibly all data in the case of WhatsApp IE⁵⁴ in order to understand whether a particular person uses different services of the Facebook Companies, would serve the interests of both WhatsApp IE and the other Facebook Companies; hence would go beyond a controller-to-processor relationship.
65. Indeed, the EDPB notes that since the combination or comparison would aim at assessing if a certain user identified as requiring action on one product or service (e.g., if they send spam or violate WhatsApp’s or Facebook’s terms and conditions) also uses Facebook Companies’ products or services (including WhatsApp IE’s), hence also face possible consequences of their acts on those other accounts, shows that, without such combination or at least comparison of both data sets, the processing would not be possible. In other words, the processing described in the FAQ “How we work with the Facebook Companies” involving actions by both WhatsApp IE and the other Facebook Companies, is inseparable, i.e. inextricably linked.
66. Considering the clear contradictions within WhatsApp’s user-facing information that should reflect the practice, as well as the contradictions between WhatsApp’s user-facing information and the statements made to the EDPB by Facebook IE and WhatsApp IE, including in their letters dated 7 July 2021, the Board considers that there is a **high likelihood that Facebook IE already processes WhatsApp user data as a controller or joint controller** for the common purpose of the safety, security and integrity of WhatsApp and the Facebook Companies.

⁵¹ See the FAQ “How we work with the Facebook Companies”, *What information does WhatsApp share with the Facebook Companies?*

⁵² See the FAQ “How we work with the Facebook Companies”, *What information does WhatsApp share with the Facebook Companies?*

⁵³ See the FAQ “How we work with the Facebook Companies”, *What information does WhatsApp share with the Facebook Companies?*

⁵⁴ See FAQ “How we work with the Facebook Companies”, How We Process Your Information > Provision Of The Services In Accordance With The Terms > Legitimate Interests > To share information with the Facebook Companies to promote safety and security and integrity > Data Categories Used: “*We use information described in the “Information You Provide,” “Automatically Collected Information,” and “Third-Party Information” sections of this Privacy Policy for this purpose.*”

67. Nonetheless, in the face of the various contradictions, ambiguities and uncertainties noted in WhatsApp's user-facing information, the Commitments, and Facebook IE and WhatsApp IE's respective written submissions, the EDPB is not in a position to determine with certainty which processing operations the other Facebook Companies, including Facebook IE, are actually carrying out in relation to WhatsApp's user data and in which capacity.
68. Accordingly, **the EDPB requests the LSA competent for Facebook IE and WhatsApp IE to carry out a statutory investigation to unveil whether Facebook IE has already started to process WhatsApp's user data for the common purpose of safety, security and integrity of the Facebook Companies, and if so, whether it is acting as a processor on behalf of WhatsApp IE or as a (joint) controller with WhatsApp IE. In particular, to this respect the LSA should analyse the possible combination and/or comparison at individual level the personal data of WhatsApp users with the data of the Facebook Companies which enables the Facebook Companies to understand whether a particular person uses different services of the Facebook Companies, which serves their common purpose of the safety, security and integrity. The EDPB further requests the LSA to carry out a statutory investigation to assess whether Facebook IE has a legal basis to conduct such processing lawfully as a (joint) controller pursuant to Articles 5(1)(a) and 6(1) GDPR.**
69. Whilst the EDPB considers that SAs enjoy a certain degree of discretion to decide how to frame the scope of their inquiries, the EDPB recalls that one of the main objectives of the GDPR is to ensure consistency throughout the EU, and the cooperation between the LSA and CSAs is one of the means to achieve this. Therefore, **the EDPB calls upon the LSA to make full use of the cooperation tools provided for by the GDPR (including Articles 61 and 62 GDPR) while carrying out such investigation.**

4.1.2.2.2 On the alleged infringement of the transparency obligations under GDPR

70. The EDPB takes note of the concerns of the DE-HH SA regarding transparency towards data subjects, in particular in relation to the processing of WhatsApp's user data for the purpose of security and safety of the Facebook Companies. However, the EDPB underlines that WhatsApp's user-facing information for EU users is currently subject to a one-stop-shop procedure led by the IE SA that is due to come to an end shortly.

4.1.3 Improvement of product experience

4.1.3.1 Summary of the position of the DE-HH SA

71. According to the DE-HH SA, it can be read in the FAQ "How we work with the Facebook Companies" that in order to understand how people use WhatsApp services in comparison with other apps and improve the WhatsApp services, WhatsApp can track the use of services and compare these results across the Facebook companies. WhatsApp may be able to match whether the user of a particular WhatsApp account also uses another Facebook company's service⁵⁵. The DE-HH SA concluded that Facebook IE's processing for its own purpose of product improvement and advertising is not presented transparently⁵⁶.
72. Moreover, according to DE-HH SA, with the new terms of use, WhatsApp is expanding the list of data to be exchanged with Facebook in the future. In particular, this relates to Facebook hosting services

⁵⁵ DE-HH SA Order, Section II.2)aa), p. 17.

⁵⁶ DE-HH SA Order, Section II.2)cc), p. 20.

and “discovering a business” features⁵⁷. According to DE-HH SA, this means that, in the future, data will also be exchanged between WhatsApp and Facebook for marketing purposes, which Facebook can use for its own purposes, in particular for profiling⁵⁸.

73. The DE-HH SA notes that the relevant section in the FAQ “How we work with the Facebook Companies” in its version before the consultation letter of the DE-HH SA of 12 April 2021 stated that Facebook does not use “account information” for purpose of improving Facebook product experience and Facebook ads⁵⁹. According to DE-HH SA, “account information” covers a very broad catalogue of information. It is not clear what is meant by “account information” and which types of data should be assigned to this data category and which should not. The DE-HH SA observes that WhatsApp collects a considerable number of other data categories.
74. The DE-HH SA further states that following the consultation letter of the DE-HH SA of 12 April 2021, the wording of “account information” in the FAQ “How we work with the Facebook Companies” has been expanded to include all personal data. The DE-HH SA notes that while previously in the FAQ “How we work with the Facebook Companies” the use of “account information” by Facebook was described by WhatsApp as “currently” not taking place, it is now only mentioned that WhatsApp is “currently” not passing on⁶⁰ (all) personal data for these purposes. Thus, the fact that Facebook IE does not actually use WhatsApp users’ data for these purposes is not (any longer) clear from the amended terms and conditions⁶¹.

⁵⁷ DE-HH SA Order, Section II.2)cc), p. 20, the relevant quote: “In the explanations it says (emphasis by the undersigned):

“Facebook hosting services: [...] Some large businesses need to use hosting services to manage their communication. Which is why we’re giving businesses the option to use secure hosting services from Facebook to manage WhatsApp chats with their customers, answer questions, and send helpful information like purchase receipts. But whether you communicate with a business by phone, email, or WhatsApp, it may use that information for its own marketing purposes, which may include advertising on Facebook. To make sure you’re informed, we clearly label conversations with businesses that are choosing to use hosting services from Facebook.

Discovering a business: You may see an ad on Facebook with a button to message a business using WhatsApp. If you have WhatsApp installed on your phone, you’ll have the option to message that business. **Facebook may use the way you interact with these ads to personalize the ads you see on Facebook.** (emphasis added by author).

Discovering a business: People can already discover businesses on Facebook or Instagram from ads that show a button you can click to message them using WhatsApp. Just like other ads on Facebook, **if you choose to click on these ads, it may be used to personalize the ads you see on Facebook.** Again, WhatsApp and Facebook cannot see the content of any end to end encrypted messages.” (emphasis added by author).

Here we would like to emphasise once again that WhatsApp and Facebook cannot see the content of end-to-end encrypted messages.” (see <https://faq.whatsapp.com/general/security-and-privacy/about-new-business-features-and-whatsapp-privacy-policy-update/?lang=en>.)”

⁵⁸ DE-HH SA Order, Section II.2)cc), p. 20.

⁵⁹ DE-HH SA Order, Section II.2)cc), p. 20.

⁶⁰ It should be noted that the exact wording from the WhatsApp Updated terms and the Commitments is “shared”.

⁶¹ DE-HH SA Order, Section II.2)cc), p. 21, the relevant quote: “However, it is no longer confirmed that Facebook does not use user data for these purposes, but only that data is not passed on for these purposes. Since then, it has only stated (emphasis added by the undersigned):

“We do not share data to use it to improve Facebook products on Facebook or to provide more relevant advertising experiences on Facebook.

Currently, WhatsApp does not share your personal data with Facebook to improve your product experience on Facebook or to show you more engaging Facebook ads. This is the result of discussions with the Irish Data Protection Authority and other data protection authorities in Europe. We are constantly working on new ways to improve your experience on WhatsApp and other Facebook company products you use. If we decide in the future

75. The DE-HH SA makes reference to Facebook's statements regarding the commitment made by WhatsApp IE not to share EU WhatsApp user data with Facebook for the purpose of Facebook using this data to improve its products or advertisements without prior consultation with the IE SA. The DE-HH SA states that this represents a non-binding commitment and requires no further user's consent⁶². The DE-HH SA also stresses that this commitment only refers to the purposes for which WhatsApp IE shares data with Facebook and does not include any commitment by Facebook not to process data for its own purposes⁶³.
76. Regarding the issue of legal basis, the DE-HH SA states that it is not clear whether WhatsApp would consider it necessary to obtain the consent of users for a transfer for these purposes. According to the DE-HH SA, it must be assumed that the transfer of its users' data to Facebook IE for these purposes on the legal basis of legitimate interest, Article 6(1)(f) GDPR⁶⁴. The DE-HH SA further states that users lack proper information about such transfers: "*In the view of both companies, the legal requirements for data transfer by WhatsApp and processing by Facebook Ireland Ltd for these purposes already exist. The consequence of this is that the users, since they are not requested to give their consent, do not obtain any secure knowledge of a data transfer for these purposes to Facebook Ireland Ltd. Rather, a data transfer for these purposes has been and is being decided and implemented by the companies "behind the scenes", whereby it is completely unclear for users whether and if so, when and in what form they will become aware of this and whether they will be asked for consent to a data transfer and processing for these purposes or will have the possibility to object to it or not*"⁶⁵.

4.1.3.2 Analysis of the EDPB

77. The EDPB assessed the improvement of product experience purpose⁶⁶ in relation to the alleged unlawful processing of WhatsApp user data by Facebook IE as a controller and in relation to the alleged infringement of the transparency requirements in WhatsApp's user-facing information. The EDPB took into account the views of the DE-HH SA, as well as the positions expressed by both Facebook IE and WhatsApp IE.

4.1.3.2.1 On the alleged unlawful processing of WhatsApp user data by Facebook IE as a controller

78. In relation to improvement of product experience, the EDPB notes the following descriptions provided in relevant extracts from WhatsApp's Privacy Policy (emphasis added underlined):

"WhatsApp also works, and shares information with, the other Facebook Companies who act on our behalf to help us operate, provide, improve, understand, customise, support, and market our

to share such data with the Facebook companies for this purpose, it will only be done if the head of the Irish data protection authority agrees to a mechanism that allows such use. We will keep you updated on new experiences we offer and our information practices."

⁶² Annex to Facebook's submissions to the DE-HH SA, para 2.4, p. 7-8, Letter to the EDPB Chair requesting a binding decision of the EDPB according to Art. 66 (2) GDPR, 3 June 2021, p. 6.

⁶³ DE-HH SA, Letter to the EDPB Chair requesting a binding decision of the EDPB according to Art. 66(2) GDPR, 3 June 2021, p. 6.

⁶⁴ DE-HH SA Order, Section II.2)cc), p. 22.

⁶⁵ DE-HH SA Order, Section II.2)cc), p. 22.

⁶⁶ This processing purpose in different parts of the DE-HH SA order is referred as "improvement of the product experience" (see the DE-HH SA order, p. 1) and/or as "Product experiences and Facebook ads" (see the DE-HH SA order, p. 20). In this section, the EDPB assesses the purpose of improvement of product experience in a broad sense. The specific advertisement related elements are addressed by the EDPB in the section 4.1.4 of the current decision.

Services. This includes the provision of infrastructure, technology, and systems, e.g., for providing you with fast and reliable messaging and calls around the world; improving infrastructure and delivery systems; understanding how our Services are used; helping us provide a way for you to connect with businesses; and securing systems. When we receive services from the Facebook Companies, the information we share with them is used on WhatsApp's behalf and in accordance with our instructions. Any information WhatsApp shares on this basis cannot be used for the Facebook Companies' own purposes⁶⁷.

79. The EDPB also notes the relevant extracts from the information included by WhatsApp in its FAQ “How we work with the Facebook Companies” (emphasis added underlined):

“Why does WhatsApp share information with the Facebook Companies?

WhatsApp works and shares information with the other Facebook Companies to receive services like infrastructure, technology, and systems that help us provide and improve WhatsApp and to keep WhatsApp and the other Facebook Companies safe and secure. When we receive services from the Facebook Companies, the information we share with them is used to help WhatsApp in accordance with our instructions. Working together allows us for example to:

- Provide you fast and reliable messaging and calls around the world and understand how our Services and features are performing.
- Ensure safety, security, and integrity across WhatsApp and the Facebook Company Products by removing spam accounts and combating abusive activity.
- Connect your WhatsApp experience with Facebook Company Products.

Today, WhatsApp does not share your personal information with Facebook to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook. We're always working on new ways to improve how you experience WhatsApp and the other Facebook Company Products you use. We'll keep you updated on new experiences we offer and our data practices⁶⁸.

[...]

“How is my WhatsApp information used by the Facebook Companies?

To receive services that will help WhatsApp operate, improve, and develop our business. When WhatsApp shares information with the Facebook Companies in these ways, the Facebook Companies act as service providers and the information we share with them is used to help WhatsApp in accordance with our instructions (emphasis added).

) We share information with the other Facebook Companies as service providers. Service providers help companies like WhatsApp by providing infrastructure, technologies, systems, tools, information, and expertise to help us provide and improve the WhatsApp service for our users.

) This enables us, for example, to understand how our Services are being used, and how it compares to usage across the Facebook Companies. By sharing information with the other Facebook Companies, such as the phone number you verified when you signed up for WhatsApp and the last time your account was used, we may be able to work out whether or not a particular WhatsApp account belongs to someone who also uses another service in the Facebook Companies. This allows us to more accurately report information about our Services and to improve our Services. So, for example, we can then understand how people use WhatsApp services compared to their use of other apps or services in the other Facebook Companies, which in turn helps WhatsApp to explore potential features or product improvements (emphasis added). We can also count how many unique users WhatsApp has, for example, by establishing which of our users do not use any other Facebook apps and how many unique users there are

⁶⁷ In the Privacy Policy (valid as of 8 February 2021), section “How we work with other Facebook Companies”.

⁶⁸ FAQ “How we work with the Facebook Companies”> How is my WA information used by the FB Companies.

across the Facebook Companies. This will help WhatsApp more completely report the activity on our service, including to investors and regulators.

[...]

We do not share data for improving Facebook products on Facebook and providing more relevant Facebook ad experiences.

) Today, WhatsApp does not share your personal information with Facebook to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook. This is a result of discussions with the Irish Data Protection Commission and other Data Protection Authorities in Europe. We're always working on new ways to improve how you experience WhatsApp and the other Facebook Company Products you use. Should we choose to share such data with the Facebook Companies for this purpose in the future, we will only do so when we reach an understanding with the Irish Data Protection Commission on a future mechanism to enable such use. We'll keep you updated on new experiences we offer and our information practices"⁶⁹.

80. The EDPB also notes the relevant extracts from the information included by WhatsApp in the Legal Basis notice (emphasis added underlined):

"Provision Of The Services In Accordance With The Terms"

We process the data we have about you (as described in the "Information We Collect" section) as necessary to perform our contract with you (the Terms). The categories of data we process will depend on the data you choose to provide and the manner in which you use our Services (which determines the information we collect automatically). The processing purposes necessary to provide our contractual services are:

Why And How We Process Your Data:

- To operate, provide, improve, customise, and support our Services as described in the "Our Services" section of our Terms which includes providing ways for you to connect and communicate with other WhatsApp users including businesses. This includes collecting information from you to create a WhatsApp account, connecting you with businesses reachable via WhatsApp, analysing your use of our Services, providing customer support in response to an issue or deleting your data if you choose to close your account.
- We use Messaging Metadata for the transmission of the communication; the operation of the Services, including general traffic management and the prevention, detection, investigation and remediation of failures; and for billing, where applicable.
- Data Categories Used: We use information described in the "Information You Provide," "Automatically Collected Information," and "Third-Party Information" sections of this Privacy Policy for this purpose.

[...]

Legitimate Interests

We rely on our legitimate interests or the legitimate interests of a third party where they are not outweighed by your interests or fundamental rights and freedoms ("legitimate interests"):

Why And How We Process Your Data:

- For providing measurement, analytics, and other business services where we are processing data as a controller.
- Legitimate Interests Relied On:

⁶⁹ See FAQ "How we work with the Facebook Companies" > How is my WA information used by the FB Companies?

- *To provide accurate and reliable aggregated reporting to businesses and other partners, to ensure accurate pricing and statistics on performance, and to demonstrate the value our partners realise using our Services; and*
- *In the interests of businesses and other partners to help them understand their customers and improve their businesses and validate our pricing models, and evaluate the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services.*
- *Data Categories Used: We use information described in the "Information You Provide," "Automatically Collected Information," and "Third-Party Information" sections of this Privacy Policy for these purposes."*

81. According to the submissions of Facebook IE, WhatsApp IE is the sole data controller: "*Facebook processes WhatsApp User Data as processor on behalf of WhatsApp Ireland*"⁷⁰ and the other Facebook companies (including Facebook IE) only process the data of WhatsApp users shared by WhatsApp IE as processors acting under WhatsApp IE instructions⁷¹. Facebook IE added that no Facebook companies, including Facebook IE, process the personal data of WhatsApp users shared by WhatsApp IE for Facebook's own purposes⁷².
82. Facebook IE noted that the alleged processing is subject to the commitment that WhatsApp IE made to WP 29 and the EU supervisory authorities that it will not share personal data of WhatsApp users in the EU with other Facebook companies for the purpose of Facebook using this data to improve its products or advertisements, and that no such use will occur without prior engagement with the IE SA in its capacity as LSA and sole interlocutor under Article 56(6) GDPR⁷³. Facebook IE provided an affidavit reaffirming the commitments and confirming that the May Update will not change the status quo⁷⁴.
83. The EDPB observes that in the Commitments WhatsApp IE, *inter alia*, committed to not commence sharing WhatsApp data relating to EU users with Facebook to improve Facebook products and advertisements, and should it change, to do so "*with continued discussion with [the IE SA]*"⁷⁵. In its submissions to the EDPB, Facebook IE claimed that this commitment is being followed by WhatsApp IE and the WhatsApp data is not being shared with Facebook for the purpose of Facebook using this data to improve Facebook products or Facebook ad experiences⁷⁶.

⁷⁰ Facebook's written submissions to DE-HH SA, section 2.11, p. 9.

⁷¹ Facebook's written submissions to DE-HH SA, sections 2.9-2.12, p. 9-10.

⁷² Facebook's written submissions to DE-HH SA, for instance section 1.1.A), p. 2.

⁷³ Facebook's written submissions to DE-HH SA, Annex 1, Letter from WhatsApp Ireland to the Article 29 Working Party dated 4 February 2018, p.1, and Letter from WhatsApp Ireland to the DPC dated 8 June 2018, p.2. In the commitments WhatsApp took towards the WP 29 and the LSA, respectively in February and June 2018, WhatsApp IE:

- _) Committed to not commence sharing WhatsApp data relating to EU users with Facebook to improve Facebook products and advertisements, and should it change, to do so "*with continued discussion with [the IE SA]*".
- _) Confirmed that Facebook will carry on providing services to WhatsApp Ireland as a processor for "*areas such as infrastructure, analytics and monetisation*".

⁷⁴ Facebook's written submissions to DE-HH SA, Annex 2.

⁷⁵ Facebook's written submissions to DE-HH SA, Annex 1, Letter from WhatsApp Ireland to the Article 29 Working Party dated 4 February 2018, p.1, and Letter from WhatsApp Ireland to the DPC dated 8 June 2018, p.2.

⁷⁶ Facebook's written submissions to the EDPB dated 25 June 2021, para. 15, 26.

84. According to Facebook IE, as the alleged processing⁷⁷ is not taking place, the statements by the DE-HH SA regarding the legal basis that WhatsApp IE or Facebook IE might rely on for such processing are not relevant to the scope of this urgency procedure. Even if they were, the DE-HH SA attempts to proactively prohibit future reliance on legal bases for future processing would be unlawful⁷⁸.
85. According to Facebook IE, the extract from the FAQ “How we work with the Facebook Companies” (see para. 80 above) is a simplified and accessible explanation of complex technical processing operations, which is designed to assist users of varying sophistication in understanding how their data is being processed by WhatsApp IE. It was not intended to provide a detailed explanation of complex legal concepts contained in the GDPR, nor can its wording provide sufficient basis on which to conclude a regulatory process on such matters. Facebook IE further stated that while it understood from WhatsApp IE that certain processing falling within this simplified description is taking place (e.g. WhatsApp Ireland is using its processor in order to establish how many unique users its service has), it is not relevant to the present proceedings for two reasons: (1) the entity providing these services to WhatsApp Ireland is in fact Facebook, Inc. and (2) Facebook, Inc. handles EU WhatsApp User Data solely as a processor on behalf of WhatsApp IE and not as a controller⁷⁹. WhatsApp IE stated the same: “[t]he entity providing the services [...] is in fact Facebook, Inc. and the processing of EU WhatsApp User Data involves Facebook, Inc. acting as a “service provider”, i.e. as a processor on behalf of WhatsApp Ireland, and not as a controller”⁸⁰.
86. Regarding the role of a processor, Facebook IE stated that “*there are no other requirements or conditions attached to the concept of a processor and no rules on the types of activities that can be undertaken or the data that can be processed. Contrary [...] the categories or sources of other data processed by an entity are clearly not relevant to determining whether an entity processes specific personal data received from a specific controller as a controller or a processor. As the EDPB acknowledges in its Draft Guidelines: “[t]wo basic conditions for qualifying as processor exist: that it is a separate entity in relation to the controller and that it processes personal data on the controller’s behalf” - both of which are applicable to the processing described in the third Extract*”⁸¹.
87. Facebook IE further claimed that “*WhatsApp Ireland is the entity that determines the purposes and means regarding the processing of EU WhatsApp User Data [...]*⁸². *Facebook Inc. handles EU WhatsApp User Data solely in accordance with WhatsApp Ireland’s instructions pursuant to both strict contractual and technical controls. Among other things, these controls prohibit Facebook, Inc. from using EU WhatsApp User Data for its own purposes, and from disclosing any such personal data to any other Facebook companies, including in particular to Facebook Ireland. The outputs of these services received by WhatsApp Ireland from Facebook, Inc. are made available in the form of aggregated information*

⁷⁷ In Facebook’s written submissions to the EDPB dated 25 June 2021, ‘Alleged Processing’ is defined by reference to the processing prohibited by the DE-HH SA Order, i.e., “[...] Facebook Ireland [...] processing personal data of WhatsApp users residing in Germany [...] transmitted by WhatsApp Ireland to Facebook Ireland as a controller, for a broadly described list of Facebook Ireland’s own purposes”, para 3.

⁷⁸ Facebook’s written submissions to DE-HH SA, p. 6, para. 1.1 (J).

⁷⁹ Facebook’s written submissions to the EDPB dated 7 July 2021, p. 5.

⁸⁰ WhatsApp’s written submissions to the EDPB dated 7 July 2021.

⁸¹ Facebook’s written submissions to the EDPB dated 7 July 2021, p. 7.

⁸² This particular section from the Facebook’s written submissions to the EDPB refers to the processing described FAQ “How we work with the Facebook Companies” > How is my WA information used by the FB Companies? (See above para. 80 of the current decision).

only. Any sharing of this information by WhatsApp Ireland with any other Facebook company could therefore not involve any sharing of EU WhatsApp User Data with that company"⁸³.

88. The EDPB firstly recalls that a processor is someone who processes personal data on the controller's behalf⁸⁴. "*Processing personal data on the controller's behalf*" firstly requires that the separate entity processes personal data *for the benefit of the controller*⁸⁵. If the separate entity processes the personal data also *for its own benefit*, that entity goes beyond the role of the processor. Moreover, the EDPB considers that a processor cannot combine data it processes on behalf of a company with other data it processes as controller without going outside its role as the processor.
89. The EDPB further notes 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)⁸⁶.
90. The EDPB recalls that the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, therefore the concept of 'controller' should be interpreted in a sufficiently broad way, favouring as much as possible effective and complete protection of data subjects so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules, while at the same time not diminishing the role of the processor⁸⁷. Further, the EDPB notes that in the analysis of processing of personal data which may be divided into several smaller processing operations and involve several actors, it is important to consider whether at "*macro-level*" these processing operations could be considered as a "set of operations" pursuing a joint purpose using jointly defined means⁸⁸.
91. According to the GDPR, a controller is "*[...] the natural or legal person, [...] which, alone or jointly with others, determines the purposes and the means of the processing of personal data*"⁸⁹, and is consequently serving its own interests⁹⁰. The EDPB recalls that "*[j]oint controllership exists when entities involved in the same processing carry out the processing for jointly defined purposes. This will be the case if the entities involved process the data for the same, or common, purposes*"⁹¹.
92. The EDPB observes that in their current drafting, the statements included in WhatsApp's public-facing information also include reference to the Commitments by providing an explanation to users that: "*WhatsApp does not share your personal information with Facebook to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook*". The EDPB also takes note of the positions of Facebook IE and WhatsApp IE that WhatsApp IE only shares the WhatsApp

⁸³ Facebook's written submissions to the EDPB dated 7 July 2021, p. 7.

⁸⁴ GDPR Article 4(8).

⁸⁵ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version, para. 78.

⁸⁶ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version, para. 12.

⁸⁷ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version, para. 14.

⁸⁸ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version, para. 43.

⁸⁹ See Article 4(7) GDPR.

⁹⁰ See by analogy, EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, final version, para 80.

⁹¹ See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 59.

user data with the other Facebook Companies for the purposes of receiving services which the other Facebook Companies provide as processors, i.e. controller to processor data sharing⁹².

93. The EDPB has serious doubts about the interpretation of the processing role of the other Facebook Companies, including Facebook IE, regarding WhatsApp user data in the present situation as claimed by Facebook IE and WhatsApp IE.
94. The EDPB notes that while the Privacy Policy and the FAQ “How we work with the Facebook Companies” are explicit that WhatsApp data is not shared with Facebook for the purpose of Facebook using this data to improve Facebook products and/or providing more relevant Facebook ad experiences, the FAQ explicitly states that the WhatsApp data is shared with Facebook to understand how WhatsApp *“Services are being used, and how it compares to usage across the Facebook Companies”*⁹³. The FAQ adds that *“we may be able to work out whether or not a particular WhatsApp account belongs to someone who also uses another service in the Facebook Companies”* and that *“[w]e can also count how many unique users WhatsApp has, for example, by establishing which of our users do not use any other Facebook apps and how many unique users there are across the Facebook Companies”*⁹⁴ (emphasis added underlined).
95. The EDPB therefore considers that the FAQ “How we work with the Facebook Companies” already incorporates elements that give indication that Facebook actions, insofar as they concern the processing of WhatsApp users’ data for the benefit of the Facebook Companies, including Facebook IE⁹⁵, go beyond the Commitments, despite the Commitments to consult the IE SA in case of any change.
96. Based on the FAQ “How we work with the Facebook Companies”, it seems apparent that the WhatsApp user data is being compared with the data of the other Facebook Companies, including Facebook IE. Moreover, considering the information provided in the FAQ “How we work with the Facebook Companies”, it could be observed that WhatsApp IE and other Facebook Companies, including Facebook IE, share with each other and possibly combine data, such as phone numbers, in order to understand whether a particular person uses different services (also referred to as “Facebook apps”) of the Facebook Companies, which include Facebook IE⁹⁶.
97. The EDPB considers that such sharing of data *“with Facebook to understand how WhatsApp Services are being used, and how it compares to usage across the Facebook Companies”* is likely done not merely for the purpose of improving the products of WhatsApp IE, but also benefits other Facebook Companies, including Facebook IE, for improvement of their products.

⁹² Facebook’s written submissions to the EDPB of 7 July 2021, p. 3, also WhatsApp’s written submissions to the EDPB of 7 July 2021.

⁹³ See FAQ “How we work with the Facebook Companies”> How is my WA information used by the FB Companies?

⁹⁴ See FAQ “How we work with the Facebook Companies”> How is my WA information used by the FB Companies?

⁹⁵ A link inserted in WhatsApp public-facing information sends to a page on WhatsApp explaining that the term ‘Facebook Companies’ refers to Facebook Inc., Facebook IE, Facebook Payments Inc., Facebook Payments International Limited, Facebook Technologies LLC, Facebook Technologies Ireland Limited, WhatsApp LLC, and WhatsApp IE. In this urgent binding decision, the term ‘other Facebook Companies’ refers to all the Facebook Companies except WhatsApp IE.

⁹⁶ For example, a link inserted in WhatsApp public-facing information sends to a page on WhatsApp explaining that the term as follows: *“The Facebook Company Products are, together, the Facebook Products and other products provided by the Facebook Companies that are subject to a separate, stand-alone terms of service and privacy policy, including the WhatsApp and Oculus Products (when using an Oculus account)”*.

98. Based on the FAQ “How we work with the Facebook Companies”, the EDPB considers it to be likely that the processing of WhatsApp user data is done for the *overall* (i.e. “*macro*”) purpose of improving products of the Facebook Companies (*inter alia*, by assessing “*which accounts across the Facebook Companies relate to the same user*” and “*how WhatsApp Services are being used, and how it compares to usage across the Facebook Companies*”). The EDPB observes that, if confirmed, such processing would go beyond the processing of WhatsApp user data for the purpose for improvement of WhatsApp products by WhatsApp IE as the only data controller.
99. The EDPB takes note of the information provided by WhatsApp IE and Facebook IE that the entity providing the above-described services to compare usage across the Facebook Companies is Facebook, Inc. and the processing of EU WhatsApp user data involves Facebook, Inc. acting as a service provider for this purpose. The EDPB raises concerns that the processing of the WhatsApp user data for the purpose for improvement of products is potentially done for the benefit of all the Facebook Companies, and not solely for WhatsApp IE own purpose of improvement of WhatsApp products.
100. Therefore, if such circumstances were to be confirmed, the Facebook Companies, including Facebook IE, potentially (jointly) define the purpose and means for this processing⁹⁷ and in such a case they should be considered as (joint) controllers in this respect⁹⁸. Accordingly, if these circumstances were confirmed, the EDPB considers that **Facebook IE could be regarded as a (joint) controller**, i.e. determining the purpose and means of processing the personal data of WhatsApp users in the EU, insofar as the processing is done for the purpose of improvement of Facebook products. However, the Board considers that based on the information available in the present procedure, it is not in a position to reach final conclusions on this matter.
101. The EDPB further considered whether, in case such processing by Facebook IE as a controller was confirmed, Facebook IE would have a **legal basis** under Article 6(1) GDPR to process the WhatsApp user data for the purpose for improvement of Facebook products lawfully pursuant to Article 5(1)(a) GDPR.
102. Regarding **consent** as a possible legal basis for such processing by Facebook IE as the controller, based on the information available to the EDPB, there is no indication that consent from users is currently collected regarding such processing⁹⁹. Therefore, the EDPB considers it unlikely that Facebook IE currently could rely on Article 6(1)(a) GDPR to lawfully conduct such processing of WhatsApp user data. The EDPB further considers that Facebook IE could not rely on **performance of contract** legal basis under Article 6(1)(b) GDPR as there is no contractual relations between the WhatsApp users and Facebook IE.
103. The EDPB has serious doubts whether Facebook IE as a (joint) controller could rely on **legitimate interest** legal basis under Article 6(1)(f) GDPR for the processing of the WhatsApp user data for the purpose of improvement of Facebook products, as in the present case the controller’s interests are likely to be overridden by the interests and fundamental rights and freedoms of the data subjects.

⁹⁷ See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 59.

⁹⁸ CJEU judgement in case C-210/16 *Wirtschaftsakademie*, 5 June 2018, para. 30.

⁹⁹ The EDPB took note that in their submissions WhatsApp IE stated several times that the consent to the new terms is not meant to constitute the consent as a legal basis for processing of personal data under the GDPR. Currently WhatsApp IE collects consent from WhatsApp service users only through the device-based settings to allow access to device information, such as for location, camera and photo, in order to provide the services described when users enable the settings. In the WhatsApp Legal Basis notice.

104. The EDPB recalls that relying on Article 6 (1)(f) GDPR requires, first, the identification of a legitimate interest pursued by the controller or by a third party, second a need to process personal data for the purposes of the legitimate interest pursued and a balancing test: the legitimate interest of the controller or third party must be balanced against the interests or fundamental rights and freedoms of the data subject¹⁰⁰. The EDPB also recalls that in order to carry out the balancing test it is first important to consider the nature and source of the legitimate interests on the one hand and the impact on the data subjects on the other hand. The legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject¹⁰¹.

105. While such type of interest, i.e. improvement of products, could be considered to be legitimate¹⁰², the EDPB stresses that this commercial interest could be less compelling when weighed against the rights of data subjects¹⁰³. Therefore, in the present case, when carrying out the balancing test, more prominent weight should be given to the consideration of interests of data subjects and the impact on their rights.

106. Taking into account the high number of WhatsApp users and the large amount of personal data¹⁰⁴ that are processed and possibly combined with other data by Facebook IE for the purpose of improvement of products of the Facebook Companies, the EDPB has serious doubts that the controller's interest would override the interests of data subjects.

107. The EDPB recalls that the reasonable expectations of the data subject, especially with regard to the use and disclosure of the data in the relevant context, is another important element to consider in the balancing test¹⁰⁵.

108. Taking into account the above, **the EDPB concludes that there is a high likelihood that Facebook IE processes WhatsApp users' data as a (joint) controller for its own purpose of improvement of product experience**. However, considering the Commitments and the submissions of Facebook IE, as well as the limited information available in this procedure, the Board concludes that it does not have sufficient information to verify whether and to what extent such processing takes places in practice and whether such processing by Facebook IE is lawful pursuant to Articles 5(1)(a) and 6(1) GDPR.

109. **Accordingly, the EDPB requests the LSA competent for Facebook IE and WhatsApp IE to carry out a statutory investigation to unveil whether Facebook IE is processing WhatsApp user data for the common purpose of improvement of products of the Facebook Companies as a (joint) controller. In particular, in this respect the LSA should investigate the processing of personal data by the Facebook Companies which enables them to identify whether a particular person uses different services of the Facebook Companies possibly facilitated by the use of unique identifiers and analyse the possible**

¹⁰⁰ EDPB Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions, adopted 19 May 2021, , para. 7-9.

¹⁰¹ Working Party 29 Opinion WP 217 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 23.

¹⁰² Working Party 29 Opinion WP 217 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 25.

¹⁰³ Working Party 29 Opinion WP 217 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 26.

¹⁰⁴ Working Party 29 Opinion WP 217 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 39.

¹⁰⁵ Working Party 29 Opinion WP 217 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 50.

combination or at least comparison of the WhatsApp users' data with data of the Facebook Companies based on the elements outlined by the EDPB in this section of the current decision.

110. The EDPB further requests the LSA to carry out a statutory investigation to assess whether Facebook IE has a legal basis to conduct such processing lawfully as a (joint) controller pursuant to Articles 5(1)(a) and 6(1) GDPR.

111. Whilst the EDPB considers that SAs enjoy a certain degree of discretion to decide how to frame the scope of their inquiries, the EDPB recalls that one of the main objectives of the GDPR is to ensure consistency throughout the EU, and the cooperation between the LSA and CSAs is one of the means to achieve this. Therefore, **the EDPB calls upon the LSA to make full use of the cooperation tools provided for by the GDPR (including Articles 61 and 62 GDPR)** while carrying out such investigation.

4.1.3.2.2 On the alleged infringement of the transparency obligations under GDPR

112. The EDPB takes note of the concerns of the DE-HH SA regarding transparency, in particular in relation to processing of WhatsApp user data for improvement of products of Facebook, possible contradictions in the privacy policy, and lack of sufficiently detailed, easily accessible and clear information. However, the EDPB underlines that the WhatsApp IE privacy policy is currently subject to a one stop shop procedure led by the IE SA.

[4.1.4 Marketing communications and direct marketing](#)

4.1.4.1 Summary of the position of the DE-HH SA

113. Another issue investigated by the DE-HH SA were changes in the Privacy Policy introduced with respect to processing of personal data for marketing purposes. According to the DE-HH SA, with the Updated Terms, WhatsApp IE is expanding the circle of data to be exchanged with Facebook in the future. In its explanations, the DE-HH SA referred to the WhatsApp FAQ page relating to its Privacy Policy (emphasis by the DE-HH SA):

Facebook hosting services: [...] Some large businesses need to use hosting services to manage their communication. Which is why we're giving businesses the option to use secure hosting services from Facebook to manage WhatsApp chats with their customers, answer questions, and send helpful information like purchase receipts. But whether you communicate with a business by phone, email, or WhatsApp, it may use that information for its own marketing purposes, which may include advertising on Facebook. To make sure you're informed, we clearly label conversations with businesses that are choosing to use hosting services from Facebook.

Discovering a business: You may see an ad on Facebook with a button to message a business using WhatsApp. If you have WhatsApp installed on your phone, you'll have the option to message that business. **Facebook may use the way you interact with these ads to personalize the ads you see on Facebook.** (emphasis added by author).

Discovering a business: People can already discover businesses on Facebook or Instagram from ads that show a button you can click to message them using WhatsApp. Just like other ads on Facebook, **if you choose to click on these ads, it may be used to personalize the ads you see on Facebook.** Again, WhatsApp and Facebook cannot see the content of any end to end encrypted messages."(emphasis added by author). Here we would like to emphasise once again that WhatsApp and Facebook cannot see the content of end-to-end encrypted messages." (see <https://faq.whatsapp.com/general/security-and-privacy/about-new-business-featuresand-whatsapp-privacy-policy-update/?lang=en>)

114. According to the DE-HH SA, this Privacy Policy entails that in the future, data will also be exchanged between WhatsApp IE and Facebook IE for marketing purposes, which Facebook IE can use for its own purposes, in particular for profiling¹⁰⁶.

115. As regards the legal basis for the processing of personal data for marketing communications and direct marketing, the DE-HH SA makes reference to the fact that WhatsApp IE claims to rely on the legitimate interests of WhatsApp IE, as well as the legitimate interests of a third party, including Facebook IE. The DE-HH SA points out that "legitimate interests" are not further differentiated despite the update on 15 May 2021¹⁰⁷. Therefore, the DE-HH SA finds it not clear whose legitimate interests would be assumed in case of marketing communications and which categories of data are used in connection with the processing for direct marketing purposes. Moreover, the DE-HH SA underlines that under "Third Party Providers", purposes are again listed that do not have to be exclusively those pursued by WhatsApp IE alone, but could also fall under the common purposes of WhatsApp IE and third parties such as Facebook, e.g. "to help you connect with businesses using our services"¹⁰⁸. In its Privacy Policy, as an example of legitimate interest, WhatsApp IE, mentions "*providing an innovative, relevant, safe, and profitable service to our users and partners*"¹⁰⁹.

116. As pointed out by the DE-HH SA¹¹⁰, in WhatsApp's privacy policy of 24 April 2018 (<https://www.whatsapp.com/legal/privacy-policyeea>), WhatsApp explained the following regarding the legal basis for marketing communications under "How we process your information" (emphasis added by the DE-HH SA):

"Our legitimate interests or the legitimate interests of a third party, unless your interests or fundamental rights and freedoms prevail ("legitimate interests"):

[...]

- *To provide you with marketing communications.*
- *These are the legitimate interests on which we rely for this processing: To promote Facebook companies' products and publish direct marketing."*

117. The DE-HH SA underlined that while WhatsApp IE referred in the past to the "publication" of direct advertising, in the Updated Terms WhatsApp IE refers to "sending" direct advertising¹¹¹. According to the DE-HH SA, this update seems to change the way and the form in which direct marketing is sent to users: *"The mailing suggests an even more targeted approach to the person concerned, especially by third parties"*¹¹².

4.1.4.2 Analysis of the EDPB

118. The EDPB assessed the marketing purpose in relation to the alleged unlawful processing of WhatsApp user data by Facebook IE as a controller, and in relation to the alleged infringement of the transparency requirements in WhatsApp's user-facing information. The EDPB took into account the views of the DE-HH SA, as well as the position expressed by both Facebook IE and WhatsApp IE.

¹⁰⁶ DE-HH SA Order, p. 20.

¹⁰⁷ DE-HH SA Order, p. 23.

¹⁰⁸ DE-HH SA Order, p. 24.

¹⁰⁹ WhatsApp's Privacy Policy, section "Our Legal Basis For Processing Data".

¹¹⁰ DE-HH SA Order, p.22.

¹¹¹ DE-HH SA Order, p.23.

¹¹² DE-HH SA Order, p.24.

4.1.4.2.1 On the alleged unlawful processing of WhatsApp user data by Facebook IE as a controller

119. After comparing the old and updated version of WhatsApp's user-facing information, the EDPB concludes that, the changes made by WhatsApp in relation to the processing of personal data for marketing communications and direct marketing are quite limited in their scope.
120. In relation to marketing, the EDPB notes the following descriptions provided in the relevant extracts from WhatsApp's Privacy Policy, in particular in the section "How We Use Information"¹¹³ (emphasis added underlined):

How We Use Information

"We use information we have (subject to choices you make and applicable law) to operate, provide, improve, understand, customize, support, and market our Services".

"Communications About Our Services And The Facebook Companies. We use information we have to communicate with you about our Services and let you know about our terms, policies, and other important updates. We may provide you marketing for our Services and those of the Facebook Companies."

How We Work With Other Facebook Companies

WhatsApp also works, and shares information with the other Facebook Companies who act on our behalf to help us operate, provide, improve, understand, customise, support, and market our Services.

Third Party Information

Third-Party Service Providers. We work with third-party service providers and the Facebook companies to help us operate, provide, improve, understand, customize, support, and market our Services

WhatsApp Provision Of The Services In Accordance With The Terms

We rely on our legitimate interests or the legitimate interests of a third party where they are not outweighed by your interests or fundamental rights and freedoms ("legitimate interests"):

Why And How We Process Your Data:

For providing measurement, analytics, and other business services where we are processing data as a controller.

• Legitimate Interests Relied On:

For providing marketing communications to you.

• Legitimate Interests Relied On: The legitimate interests we rely on for this processing are: To promote Facebook Company Products and send direct marketing.

121. WhatsApp's Privacy Policy clearly indicates WhatsApp IE uses data to provide marketing for its services and those of Facebook Companies. This element does not per se imply its sharing of data to Facebook IE, with Facebook IE acting as data controller.

¹¹³ <https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en> .

122. The EDPB takes into account also Facebook IE's position, which informed the DE-HH SA that, although WhatsApp's Privacy Policy enables it to engage in sending direct marketing to WhatsApp's EU users, to promote WhatsApp IE's or Facebook IE's products and services, it currently does not do it in practice and that "*It is included in the Privacy Policy should WhatsApp IE decide to commence this processing (which is a standard form of processing for most companies) in the future*"¹¹⁴.

123. On the basis of the above excerpts from WhatsApp's user-facing information, it can also be concluded that WhatsApp IE works with third parties and the other Facebook Companies for marketing purposes. However, there is not enough evidence to prove that the exchange of data is taking place and that in the context of such alleged processing, Facebook IE acts as a controller or a joint controller. At the same time, it should be underlined that WhatsApp's user-facing information refers to the legitimate interest of third parties as the legal basis and does not explicitly exclude the possibility of sharing of data with Facebook IE for the latter's direct marketing purposes.

124. Based on the information provided by the DE-HH SA, as well as WhatsApp IE and Facebook IE's written submissions, it can be concluded that in relation to the processing of personal data for marketing communications and direct marketing, Facebook IE is planning to act, at least as a processor, on behalf of WhatsApp IE. At the same time, the information analysed by the EDPB does not reveal that a data exchange is currently taking place and that Facebook IE processes data of WhatsApp's users for its own marketing purposes. However, the description of the services and of the roles provided in WhatsApp's user-facing information is not clear. This matter thus requires further investigation.

125. In conclusion, the EDPB understands the concerns raised by the DE-HH SA on the need to closely analyse the roles and legal qualification of the parties involved in the processing of WhatsApp's user data for marketing purposes. However, the EDPB does not have sufficient information in the present procedure to conclude whether Facebook IE is acting as a controller of WhatsApp user data for the purpose of marketing communication and direct marketing.

126. Taking into consideration the lack of clarity in the information part of the file as regards how data are processed, **the EDPB calls upon the IE SA to further investigate the role of Facebook IE, i.e. whether Facebook IE acts a processor or as a (joint controller), with respect to the processing of WhatsApp user personal data for marketing purposes, taking into due account the matters indicated above by the EDPB.**

4.1.4.2.2 On the alleged infringement of the transparency obligations under GDPR

127. The EDPB takes note of the concerns of the DE-HH SA regarding the transparency requirements, in particular in relation to the processing of data for marketing purposes and the fact that WhatsApp's user-facing information is not transparent on which categories of data are used for the marketing communications¹¹⁵. However, the EDPB underlines that WhatsApp IE's user-facing information is currently subject to a one stop shop procedure led by the IE SA that is due to come to an end shortly.

[*4.1.5 WhatsApp Business API*](#)

4.1.5.1 Summary of the position of the DE-HH SA

128. The DE-HH SA notes that WhatsApp's user data are also processed, or may be processed, for the general purpose of providing the so-called "WhatsApp Business API". "WhatsApp Business API"

¹¹⁴ Facebook IE response to the DE-HH SA hearing before issuing the DE-HH SA Order of 10 May 2021, dated 25 April 2021, p.12-13.

¹¹⁵ DE-HH SA Order, p. 24.

enables companies to use WhatsApp in their corporate communication systems and to communicate with their contacts and customers. Those companies may rely on third party hosting services to manage their messaging function on their behalf. Facebook IE plans to start offering the WhatsApp Business API service later this year¹¹⁶, i.e. it would host and operate a WhatsApp business client, something that, according to Facebook IE, other service providers already do¹¹⁷.

129. Facebook IE assured the DE-HH SA that these services would not be offered under the Updated Terms coming into effect, and committed to not launch them in Germany (or the EU) without an additional briefing of the IE SA, in its capacity as LSA.¹¹⁸

130. According to Facebook IE, the Updated Terms aim to clarify *inter alia* that Facebook IE will, in the future, be one of the service providers that businesses can choose from when implementing the WhatsApp Business API¹¹⁹. Facebook IE underlined that the hosting and operation of a WhatsApp business client by Facebook IE will be completely optional for businesses and will be offered by Facebook IE to businesses in a manner whereby Facebook IE will act as a processor on behalf of and under the instructions of such business customers¹²⁰. Furthermore, according to Facebook IE, it is clear from WhatsApp's encryption FAQ¹²¹ that the business becomes a controller of any messages it receives from its customers on WhatsApp and that "*it is the business' responsibility to comply with any applicable legal requirements and terms*"¹²².

131. According to the DE-HH SA, the data protection regulations concerning Facebook Business Tools, i.e. the Facebook Controller Addendum¹²³, regulate the joint responsibility between the companies and Facebook IE¹²⁴. The DE-HH SA notes that WhatsApp, in its Business Data Processing Terms¹²⁵, considers the use of the WhatsApp Business API as a contract processing¹²⁶. However, since WhatsApp offers businesses their presence on WhatsApp, which is comparable to a Facebook page, the DE-HH SA considered that a joint controllership should be applied, in light of the CJEU rulings *Wirtschaftsakademie* and *Fashion ID*¹²⁷.

132. The DE-HH SA notes that Facebook IE receives, via Facebook Business Tools, business tool data in the form of impression data sent from Facebook social plugins (such as the "Like" and "Share" buttons) and from Facebook Login, as well as from certain APIs such as Messenger Customer Match via the Send API¹²⁸.

133. According to the DE-HH SA, once Facebook IE starts helping businesses to set up, host, and operate a WhatsApp business client (WhatsApp Business API), "*WhatsApp users' communications with*

¹¹⁶ Facebook's written submissions to the DE-HH SA, p. 14, para. 2.31.

¹¹⁷ Facebook's written submissions to the DE-HH SA, p. 14, para. 2.31; Facebook's written submissions to the EDPB dated 25 June 2021, p. 26, para. 37.

¹¹⁸ Facebook's written submissions to the DE-HH SA, section 1.1, G, p. 5; Facebook's written submissions to the EDPB dated 25 June 2021, footnote 31.

¹¹⁹ Facebook's written submissions to the DE-HH SA, p. 14, para. 2.32.

¹²⁰ Facebook's written submissions to the DE-HH SA, p. 14, para. 2.31.

¹²¹ <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption>.

¹²² Facebook's written submissions to the DE-HH SA, p. 15, para. 2.32.

¹²³ https://www.facebook.com/legal/controller_addendum.

¹²⁴ DE-HH SA Order, Section II.2) ee), p. 24.

¹²⁵ <https://www.whatsapp.com/legal/business-data-processing-terms>

¹²⁶ <https://www.whatsapp.com/legal/business-data-processing-terms>

¹²⁷ The DE-HH SA refers to CJEU, C-210/16, *Wirtschaftsakademie*, ECLI:EU:C:2018:388 and C-40/17, *Fashion ID*, ECLI:EU:C:2019:629.

¹²⁸ <https://www.facebook.com/legal/terms/businesstools/>

companies that can be reached on WhatsApp will become available to Facebook in plain text without end-to-end encryption".¹²⁹ The DE-HH SA is of the opinion that the way in which WhatsApp IE refers to these circumstances in its Updated Terms is "non-transparent" and "partly contradictory"¹³⁰.

134. The DE-HH SA considers that it is unclear from the wording of WhatsApp's FAQ page¹³¹ summarising information about the Updated Terms that "personal conversations" protected by end-to-end encryption include only those that are not conducted with companies via a vendor and not all conversations of private users¹³².

135. According to the DE-HH SA, from the terms of the WhatsApp Privacy Policy¹³³, "*it is hardly discernible that with regard to a communication with companies using the WhatsApp business client, there is no end-to-end encryption of the messages and Facebook Ireland Ltd. can be granted access to information on messages and their content*". The DE-HH SA quotes in particular parts of WhatsApp's Privacy Policy ('Information You Provide') where it is stated that WhatsApp IE does not retain users' messages in the ordinary course of providing its services, but there is a description of two situations where WhatsApp IE may store its users' messages in the course of delivering them, i.e. for undelivered messages and media forwarding¹³⁴. The DE-HH SA then compared this information with the information provided by WhatsApp on its Encryption FAQ webpage under the title "About end-to-end encryption", and more specifically, to the sections entitled "Personal Messaging" and "Business Messaging"¹³⁵. The DE-HH SA considered that "*for WhatsApp users, it remains unclear in which situations their personal data and message content are processed by Facebook Ireland Ltd*" because "*different, sometimes contradictory information is communicated to them at different levels*"¹³⁶.

136. Furthermore, according to the DE-HH SA, it is not apparent to WhatsApp IE's users when they communicate with Facebook IE as a vendor, and whether their data found in the specific communication can be used for advertisements on Facebook¹³⁷. The DE-HH SA was of the opinion that WhatsApp IE "*ultimately intends, on the basis of its amended terms of service, to transmit message content to Facebook Ireland Ltd. with the purpose of enabling Facebook Ireland Ltd. to personalise advertisements*" and referred to Facebook IE and WhatsApp IE as to "*both data controllers*".¹³⁸

137. The DE-HH SA reached the conclusion that it was not made transparent to WhatsApp's users that the processing operations of WhatsApp IE and Facebook IE will "*merge even more with each other through the new business model*"¹³⁹ and that the legal basis for such data processing by Facebook IE was not sufficiently clear from the Updated Terms.

138. According to Facebook IE, the allegation that WhatsApp IE plans to share message content with Facebook IE to enable the personalisation of advertising on Facebook cannot be derived from the wording of the FAQ on encryption and ensures that every message sent on WhatsApp uses the same industry leading signal protocol that protects messages from before they are sent until they are

¹²⁹ DE-HH SA Order, Section II.2) ee), p. 25

¹³⁰ DE-HH SA Order, Section II.2)ee), p. 25, para. 2.

¹³¹ <https://faq.whatsapp.com/general/security-and-privacy/were-updating-our-terms-and-privacy-policy/>

¹³² DE-HH SA Order, Section II.2)ee), p. 25, para. 3.

¹³³ <https://www.whatsapp.com/legal/updates/privacy-policy-eea> (footnote 25 of the De-HH SA Order)

¹³⁴ DE-HH SA Order, Section II.2)ee), pp. 25-26.

¹³⁵ <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/>

¹³⁶ DE-HH SA Order, Section II.2)ee), p. 26.

¹³⁷ DE-HH SA Order, Section II.2)ee), p. 27.

¹³⁸ DE-HH SA Order, Section II.2)ee), p. 26.

¹³⁹ DE-HH SA Order, Section II.2)ee), p. 26, last para.

delivered to the intended recipient, meaning that WhatsApp IE cannot grant access to Facebook IE or any other third party to such content¹⁴⁰.

4.1.5.2 Analysis of the EDPB

139. The EDPB assessed the WhatsApp Business API purpose in relation to the alleged unlawful processing of WhatsApp IE's user data by Facebook IE as a controller, as well as in relation to the alleged infringement of the transparency requirements in WhatsApp's user-facing information. The EDPB took into account the views of the DE-HH SA, as well as the position expressed by both Facebook IE and WhatsApp IE.

4.1.5.2.1 On the alleged unlawful processing of WhatsApp user data by Facebook IE as a controller

140. The EDPB analysed the documents referred to in the DE-HH SA Order with regard to the alleged unlawful processing of WhatsApp's user data by Facebook IE as a controller for the provision of WhatsApp Business API.

141. The EDPB notes that WhatsApp's Privacy Policy provides the following information (emphasis added underlined):

"How we use information

[...] Business Interactions. We enable you and third parties, like businesses, to communicate and interact with each other using our services, such as Catalogs for businesses on WhatsApp through which you can browse products and services and place orders. Businesses may send you transaction, appointment, and shipping notifications; product and service updates; and marketing. For example, you may receive flight status information for upcoming travel, a receipt for something you purchased, or a notification when a delivery will be made. Messages you receive from a business could include an offer for something that might interest you. We do not want you to have a spammy experience; as with all of your messages, you can manage these communications, and we will honor the choices you make.

Information You And We Share

[...] Businesses On WhatsApp. We offer specific services to businesses such as providing them with metrics regarding their use of our services.

Third-Party Information

[...] Businesses On WhatsApp. Businesses you interact with using our Services may provide us with information about their interactions with you. We require each of these businesses to act in accordance with applicable law when providing any information to us.

When you message with a business on WhatsApp, keep in mind that the content you share may be visible to several people in that business. In addition, some businesses might be working with third-party service providers (which may include Facebook) to help manage their communications with their customers. For example, a business may give such third-party service provider access to its communications to send, store, read, manage, or otherwise process them for the business. To understand how a business processes your information,

¹⁴⁰ Facebook's written submissions to the DE-HH SA, p. 14 para. 2.29 and 2.30.

including how it might share your information with third parties or Facebook, you should review that business' privacy policy or contact the business directly.

Information you provide

[...] We offer end-to-end encryption for our Services. End-to-end encryption means that your messages are encrypted to protect against us and third parties from reading them. Learn more about end-to-end encryption and how businesses communicate with you on WhatsApp. [...]

142. The EDPB also considered the information provided on WhatsApp's IE FAQ page which summarises the changes made to the Updated Terms. The following extract is quoted by the DE-HH SA in the DE-HH SA Order¹⁴¹ (emphasis added underlined):

"[...] Our commitment to your privacy isn't changing. Your personal conversations are still protected by end-to-end encryption, which means no one outside of your chats, not even WhatsApp or Facebook, can read or listen to them.¹⁴² [...]"

143. In addition, the EDPB takes note of the following extract which can be read on WhatsApp FAQ Page "About end-to-end encryption"¹⁴³ (emphasis added underlined):

Personal Messaging

WhatsApp's end-to-end encryption is used when you chat with another person using WhatsApp Messenger. End-to-end encryption ensures only you and the person you're communicating with can read or listen to what is sent, and nobody in between, not even WhatsApp. This is because with end-to-end encryption, your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. All of this happens automatically: no need to turn on any special settings to secure your messages.

Business Messaging

Every WhatsApp message is protected by the same Signal encryption protocol that secures messages before they leave your device. When you message a WhatsApp business account, your message is delivered securely to the destination chosen by the business.

WhatsApp considers chats with businesses that use the WhatsApp Business app or manage and store customer messages themselves to be end-to-end encrypted. Once the message is received, it will be subject to the business's own privacy practices. The business may designate a number of employees, or even other vendors, to process and respond to the message.

Some businesses will be able to choose WhatsApp's parent company, Facebook, to securely store messages and respond to customers. While Facebook will not automatically use your messages to inform the ads that you see, businesses will be able to use chats they receive for their own marketing purposes, which may include advertising on Facebook. You can always contact that business to learn more about its privacy practices.

¹⁴¹ WhatsApp's FAQ page referred to by the DE HH-SA in the DE-HH SA Order, p. 25.

¹⁴² <https://faq.whatsapp.com/general/security-and-privacy/were-updating-our-terms-and-privacy-policy/>. The DE-HH SA uses a translation of this extract which is slightly different than the original English version (DE-HH SA Order, Section II.2) ee), p. 25).

¹⁴³ <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/> referred to by the DE HH-SA in the DE-HH SA Order, p. 26.

144. The EDPB took into account the allegations of the DE-HH SA, as well as the views expressed by both Facebook IE and WhatsApp IE.
145. The EDPB notes that despite the wording already provided in WhatsApp's public-facing information, Facebook IE indicated that Facebook IE is not providing the WhatsApp Business API service yet and plans to start offering it later this year¹⁴⁴. In addition, the EDPB takes note of the fact that Facebook IE committed, both in its submissions to the DE-HH SA before the issuing of the provisional measures and in its submissions to the EDPB, that it will not launch the service in the EU without prior consultation with the LSA and that, in any event, Facebook IE would only act as a processor on behalf of the businesses using the WhatsApp Business API service¹⁴⁵.
146. In conclusion, the EDPB understands the concerns raised by the DE-HH SA on the need to closely analyse the roles and legal qualification of the parties. The Board is concerned that a potential merging of the WhatsApp IE and Facebook IE processing operations and infrastructures for the provision of WhatsApp Business API would in practice lead to Facebook IE processing of WhatsApp's user data for its own purposes, such as for personalising advertisements. Bearing in mind that Facebook's business model is to a large extent based on advertising, the Board takes the view that the LSA should further closely investigate the roles that WhatsApp IE, Facebook IE and the businesses concerned would play in the context of the WhatsApp Business API in order to verify their compliance with the GDPR.

147. However, the Board considers that, at this stage, it does not have sufficient information in the present procedure to establish with certainty that Facebook IE already started or will soon start processing WhatsApp's user data in the context of the WhatsApp Business API service as a controller.
148. Therefore, **the Board calls upon the LSA to assess the role of Facebook IE, i.e. whether Facebook IE acts a processor or as a (joint controller), with respect to the processing of WhatsApp user personal data in the context of the WhatsApp business API. The LSA should further analyse the situations in which businesses decide to rely on Facebook for advertisements and determine whether Facebook IE, when using the content of messages sent via WhatsApp to businesses, would be acting as (joint) controller.**

4.1.5.2.2 On the alleged infringement of the transparency obligations under GDPR

149. The EDPB would first like to stress the lack of consistency between the assurance provided by Facebook IE to not launch this process without an additional briefing of the IE SA, in its capacity as LSA¹⁴⁶ and the content of WhatsApp's user-facing information, which should provide reliable, up-to-date information and reflect WhatsApp IE and Facebook IE's current roles in the provision of the WhatsApp Business API.
150. The EDPB takes note of the concerns of the DE-HH SA regarding the transparency requirements, in particular in relation to the WhatsApp Business API services. However, the EDPB underlines that WhatsApp's public-facing information is currently subject to a one-stop-shop procedure led by the IE SA due to come to an end soon.

¹⁴⁴ Facebook's written submissions to the DE-HH SA, section 2.31, p. 14.

¹⁴⁵ Facebook written submissions to the DE-HH SA, section 1.1, G, p.5; Facebook's written submissions to the EDPB dated 25 June 2021, footnote 31.

¹⁴⁶ Facebook's written submissions to the DE-HH SA, section 1.1, G, p. 5; Facebook's written submissions to the EDPB dated 25 June 2021, footnote 31.

4.1.6 Cooperation with other Facebook Companies

4.1.6.1 Summary of the position of the DE-HH SA

151. The DE-HH SA notes that WhatsApp IE, in its public-facing information, claims that when it receives services from the other Facebook Companies, WhatsApp IE's user data are processed by the other Facebook Companies on behalf of WhatsApp IE and according to its instructions¹⁴⁷. However, the DE-HH SA considered that "*The extent to which data is transferred and processed by Facebook Ireland Ltd. for the various purposes is not clear from the terms and conditions*". Besides, the DE-HH SA noted that the condition "*when we receive services from other Facebook Companies*" remains unclear and "*obviously does not refer to cases in which the exchange of data takes place for common purposes or for the purposes of the other Facebook companies*".¹⁴⁸
152. The DE-HH SA is of the opinion that due to the wording "*some device information*" and "*some of your usage information*" it is unclear which categories of data are concerned, and it is also unclear why the aforementioned data processed by Facebook IE are needed for the purpose of receiving services from the other Facebook Companies.¹⁴⁹ The DE-HH SA also noted that "*After all, this includes the phone number and account and device information, which are only mentioned by way of example, suggesting that further personal data is shared*"¹⁵⁰.
153. According to the DE-HH SA, it can be reasonably assumed, on the basis of the statements included in WhatsApp's public-facing information, that a number - if not all - personal data collected by WhatsApp IE on its users are already shared or could be shared at any time and used across the other Facebook Companies, including by Facebook IE, for their own purposes¹⁵¹, including for cooperation.

4.1.6.2 Analysis of the EDPB

154. The EDPB assessed the cooperation with the other Facebook Companies purpose in relation to the alleged unlawful processing of WhatsApp's user data by Facebook IE as a controller, as well as in relation to the alleged infringement of the transparency requirements in WhatsApp's user-facing information. The EDPB took into account the views of the DE-HH SA, as well as the position expressed by both Facebook IE and WhatsApp IE.

4.1.6.2.1 On the alleged unlawful processing of WhatsApp user data by Facebook IE as a controller

155. The EDPB notes that WhatsApp's FAQ "How we work with the Facebook Companies" provides the following information:

"Why does WhatsApp share information with the Facebook Companies?"

WhatsApp works and shares information with the other Facebook Companies to receive services like infrastructure, technology, and systems that help us provide and improve WhatsApp and to keep WhatsApp and the other Facebook Companies safe and secure. When we receive services from the Facebook Companies, the information we share with them is used to help WhatsApp in accordance with our instructions. Working together allows us for example to:

¹⁴⁷ DE-HH SA Order, Section II.2)aa), p. 16. and p. 18 refers to WhatsApp Privacy Policy's section "How We Work With Other Facebook Companies".

¹⁴⁸ DE-HH SA Order, Section II.2)aa), p. 18.

¹⁴⁹ DE-HH SA Order, Section II.2)aa), p. 17.

¹⁵⁰ DE-HH SA Order, Section II.2)aa), p. 17.

¹⁵¹ DE-HH SA Order, Section II.2)aa), p. 16.

-) Provide you fast and reliable messaging and calls around the world and understand how our Services and features are performing.
-) Ensure safety, security, and integrity across WhatsApp and the Facebook Company Products by removing spam accounts and combating abusive activity.
-) Connect your WhatsApp experience with Facebook Company Products.

What information does WhatsApp share with the Facebook Companies?

In order to receive services from the Facebook Companies, WhatsApp shares the information we have about you as described in the “Information We Collect” section of the Privacy Policy. For example, to provide WhatsApp with analytics services, Facebook processes the phone number you verified when you signed up for WhatsApp, some of your device information (your device identifiers associated with the same device or account, operating system version, app version, platform information, your mobile country code and network code, and flags to enable tracking of the update acceptance and control choices), and some of your usage information (when you last used WhatsApp and the date you first registered your account, and the types and frequency of your features usage) on WhatsApp’s behalf and in accordance with our instructions. [...]

Whose WhatsApp information is shared with the Facebook Companies for these purposes?

We share information for all WhatsApp users if they choose to use our Services. This may include those WhatsApp users who are not Facebook users because we need to have the ability to share information for all of our users, if necessary, in order to be able to receive valuable services from the Facebook Companies and fulfill the important purposes described in our Privacy Policy and this article.

In all cases, we share the minimum amount of information that is needed to fulfill these purposes. We also ensure that the information we share is up to date, so if you choose to update your WhatsApp phone number, for example, that number will also be updated by the members of the Facebook family who have received it from us.

Importantly, WhatsApp does not share your WhatsApp contacts with Facebook or any other members of the Facebook Companies for use for their own purposes, and there are no plans to do so.”

156. The EDPB also took into account the following extracts from WhatsApp's Privacy Policy:

“Information We Collect

WhatsApp must receive or collect some information to operate, provide, improve, understand, customize, support, and market our Services, including when you install, access, or use our Services. The types of information we receive and collect depend on how you use our Services. [...]

How We Work With Other Facebook Companies

“When we receive services from the Facebook Companies, the information we share with them is used on WhatsApp’s behalf and in accordance with our instructions. Any information WhatsApp shares on this basis cannot be used for the Facebook Companies’ own purposes.

We’ve set out further information in our Help Center about how WhatsApp works with the Facebook Companies.”

157. The EDPB further notes that in its Order the DE-HH SA quoted the following extracts from Facebook's privacy statement¹⁵²:

"How do Facebook companies work together?

"Facebook and Instagram share infrastructure, systems and technology with other Facebook companies (including WhatsApp and Oculus) to deliver an innovative, relevant, consistent and secure experience across all of the Facebook companies' products that you use. For these purposes, we also process information about you across Facebook companies as permitted by applicable law and in accordance with their terms and policies. For example, we process information from WhatsApp regarding accounts that send spam on the service so that we can take appropriate action against such accounts on Facebook, on Instagram or in Messenger. We also try to find out how people use and interact with Facebook companies' products, for example to find out about the number of individual users on different Facebook companies' products."

Regarding the term "Facebook company", Facebook states¹⁵³:

"In addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates all of the companies listed below in accordance with their respective terms of service and privacy policies. We may share information about you within our group of companies in order to facilitate, support and integrate their activities and to improve our services.

For more information about the privacy practices of Facebook companies and how they handle user information, please see the links below:

-) Facebook Payments Inc. (https://www.facebook.com/payments_terms/privacy) and Facebook Payments International Limited (https://www.facebook.com/payments_terms/EU_privacy)
-) Onavo (http://www.onavo.com/privacy_policy)
-) Facebook Technologies, LLC and Facebook Technologies Ireland Limited (<https://www.oculus.com/store-dp/>).
-) WhatsApp Inc. and WhatsApp Ireland Limited (<http://www.whatsapp.com/legal/#Privacy>).
-) CrowdTangle (<https://www.crowdtangle.com/privacy>)"

158. The EDPB concludes that, for the processing described by the DE-HH SA, there are not enough elements allowing to conclude that Facebook IE is processing or is going to process WhatsApp's user data for its own purposes. While Facebook IE, in its submissions to the EDPB, explicitly states that the alleged processing is not taking place, the DE-HH SA fails to provide concrete arguments proving the contrary and does not sufficiently identify the processing at stake.

159. However, due to the lack of sufficient clarity and transparency in WhatsApp's public-facing information, the EDPB considers it to be extremely difficult, if not impossible, to have a complete overview of the purposes of processing made under the framework for cooperation with the other Facebook Companies (additional to the ones already identified by the EDPB under Sections 4.1.2, 4.1.3., 4.1.4. and 4.1.5) and to verify whether Facebook IE only acts as a processor on behalf of WhatsApp IE for those purposes.

160. Therefore, the **Board calls upon the LSA to carry out an investigation to clarify the processing for the purpose of cooperation with the other Facebook Companies and to analyse the processing roles of**

¹⁵² DE-HH SA Order, Section II.2)ee), p. 15.

¹⁵³ <https://www.facebook.com/help/111814505650678?ref=dp>. DE-HH SA Order, footnote 10, p. 15.

different parties involved, in particular to verify whether Facebook IE acts a processor or as a (joint controller) with respect to such processing of WhatsApp user personal data

4.1.6.2.2 On the alleged infringement of the transparency obligations under GDPR

161. Although it cannot be established that Facebook IE acts as a controller for the purpose of cooperation with other Facebook Companies, the EDPB shares the DE-HH SA's concerns on the lack of clarity and transparency in WhatsApp's user-facing information.
162. However, the EDPB underlines that WhatsApp's public-facing information is currently subject to a one-stop-shop procedure led by the IE SA due to come to an end soon.

4.1.7 Conclusion

163. The EDPB considers that it **does not have sufficient information** in the present procedure to conclude whether infringements are taking place.

4.2 On the existence of urgency to adopt final measures by way of derogation from the cooperation and consistency mechanisms

164. The second main element to assess on the need for the EDPB to order the adoption of final measures is **the existence of an urgent situation for the protection of the rights and freedoms of data subjects, which requires the application of Article 66(2) GDPR by way of derogation from the regular consistency and cooperation mechanisms**.
165. The possible urgent intervention of the EDPB under Article 66(2) GDPR is exceptional and derogates from the general rules applicable to the consistency or cooperation mechanisms, such as the one-stop-shop procedure.
166. In the present procedure, the EDPB has to urgently decide and possibly request an SA to adopt final measures to be imposed on a controller or processor. Conversely, the one-stop-shop procedure provides some time for the LSA and CSAs to cooperate before the LSA's preparation of its draft decision and during the consultation phases provided under paragraphs 4 and 5 of Article 60 GDPR.
167. Considering the fact that the urgency procedure under Article 66(2) GDPR is a derogation to the standard consistency and cooperation mechanisms, it must be interpreted restrictively. Therefore, the EDPB will request final measures under Article 66(2) only if the regular cooperation or consistency mechanisms cannot be applied in their usual manner due to the urgency of the situation.
168. According to Recital 137 GDPR "*there may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded*". While this recital relates to provisional measures based on Article 66(1) GDPR, the adoption of final measures pursuant to Article 66(2) GDPR also requires the existence of urgency, even if the threshold to establish the urgency in that case is higher than in Article 66(1) GDPR situations.
169. The EDPB further considers that the nature, gravity and duration of an infringement, as well as the number of data subjects affected and the level of damage suffered by them, may play an important part when deciding whether or not there is an urgent need to act in a particular case.

170. The GDPR provides for two situations for which the urgency is presumed and does not have to be demonstrated, namely in accordance with Article 62(7) GDPR and Article 61(8) GDPR. The EDPB will therefore first examine whether a legal presumption is applicable in this particular case, and if not, whether there is the existence of urgency in the case at hand.

4.2.1 Possible application of a legal presumption of urgency justifying the need to derogate from the cooperation and consistency mechanisms

4.2.1.1 Summary of the position of the DE-HH SA

171. The DE-HH SA considers that Article 61(8) GDPR is applicable in this case¹⁵⁴. Under Article 61(8) GDPR, an urgency is presumed when the SA subject to an information and mutual assistance request from another SA has not provided the information required by Article 61(5) GDPR within one month.

172. In the case at hand, the IE SA shared the Updated Terms with the CSAs on 8 December 2020 using the IMI system, which gave rise to various follow-up questions that the DE-HH SA and other CSAs asked the IE SA in the IMI system. According to the DE-HH SA, the IE SA responded to the DE-HH SA's letter of 14 January 2021 "*by forwarding all the questions asked*" by the CSAs to WhatsApp IE "*and playing back WhatsApp's answers. The IE SA did not communicate its own position on the [DE-HH SA's] questions or WhatsApp IE's answers*¹⁵⁵".

173. The DE-HH SA responded to this with a letter to the IE SA on 12 February 2021 and urged the IE SA, as the LSA, to conduct its own investigations in order to clear up various ambiguities that remained even after the letter of WhatsApp IE of 5 February 2021. The DE-HH SA underlined that WhatsApp IE and Facebook IE "*are sharing data for different purposes of each company*¹⁵⁶" and that "*a legal ground for this cannot be seen*¹⁵⁷". The DE-HH SA explicitly pointed out that "*in case no deeper inspection was carried out by the [IE SA] as lead authority, we give notice of the possibility of an urgency procedure pursuant to Art. 66 GDPR*¹⁵⁸".

174. However, according to the DE-HH SA, "*there was no reaction to this request in the form of a statement by the [IE SA] or the opening of an investigation. Rather, the [IE SA] was content of forwarding the letters of various supervisory authorities and with sharing the response letters. The [IE SA] forwarded WhatsApp response letter of 24 February 2021 without comments. Even after a last request from [the DE-HH SA] on 4 March 2021, the [IE SA] did not comment on whether or not it intended to initiate a corresponding investigation*¹⁵⁹". According to the DE-HH SA's formal request to the EDPB to adopt an urgent binding decision, the IE SA did not respond to that date to the DE-HH SA's request to investigate the actual processing operations and data exchange between WhatsApp IE and Facebook IE.

175. In sum, in view of the DE-HH SA, the urgency of the case must therefore already be presumed based on procedural reasons: the DE-HH SA considers to have sent a large number of questions regarding the Updated Terms to the LSA within the framework of the mutual assistance procedure initiated by the IE SA, without having received a response from the IE SA within the meaning of Article 61(5) of the GDPR.

¹⁵⁴ DE-HH SA's letter of 3 June 2021 to the EDPB Chair, requesting an urgent binding decision pursuant to Article 66(2) GDPR, p. 9.

¹⁵⁵ DE-HH SA Order, p. 12.

¹⁵⁶ DE-HH SA's letter of 12 February 2021 to the IE SA.

¹⁵⁷ *Ibidem.*

¹⁵⁸ *Ibidem.*

¹⁵⁹ DE-HH SA Order, p. 12.

4.2.1.2 EDPB analysis

176. Article 61(9) GDPR provides the possibility for the European Commission (hereinafter the “EC”) to specify, by means of implementing acts, the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between SAs. On 16 May 2018, the EC adopted an implementing act relating to the use of the EC Internal Market Information system for GDPR consistency and cooperation procedures, including for Article 61 GDPR mutual assistance requests (IMI system).¹⁶⁰
177. The IMI system provides for a procedure relating to formal Article 61 GDPR requests, technically implementing the legal deadline of one month to reply. Following a request made by the EDPB members, the IMI system also includes a procedure relating to “Voluntary Mutual Assistance requests” (“VMA requests”). This procedure allows an SA to informally ask to or share information with the other SAs (in accordance with Article 57(1)(g) GDPR). Unlike formal Article 61 GDPR requests, the SA receiving a VMA request does not have a legal obligation to answer to that request.
178. The EDPB notes that all the communications between the LSA and the DE-HH SA were made by using the procedure for VMA requests. This VMA request was first initiated by the IE SA when it shared the Updated Terms on 8 December 2020 with the CSAs, and all the further exchanges between the LSA and the DE-HH SA were made within this framework. The DE-HH SA did not formally launch an Article 61 GDPR request in the IMI system to the LSA, but merely sent a letter replying to the VMA request flow initiated by the IE SA.
179. Furthermore, following the DE-HH SA’s hearing letter sent to Facebook IE on 12 April 2021, the LSA wrote on 19 April 2020 to the CSAs to inform them that in its view, “[...] *the substance of the text of the revised WhatsApp [IE] privacy policy is largely a carryover of the text of the existing policy and no new text signifying any change in WhatsApp’s position is included regarding the sharing of WhatsApp user data with Facebook or access by Facebook for Facebook’s own purposes*”. The IE SA also informed the CSAs that “*in March 2021 the DPC commenced a supervision review and assessment of WhatsApp Ireland’s oversight and monitoring of its data processors (chiefly Facebook), including the safeguards, mechanisms and audit processes in place to ensure that Facebook does not use WhatsApp Ireland user data for its own purposes, inadvertently or otherwise*”.
180. In light of the above, the EDPB considers that the DE-HH SA has not demonstrated that the LSA failed to provide information in the context of a formal request for mutual assistance under Article 61 GDPR.
181. **The EDPB therefore considers that Article 61(8) GDPR is not applicable in this specific case. Accordingly, the urgent nature of the DE-HH SA’s Article 66(2) GDPR request cannot be presumed and needs to be demonstrated.**

4.2.2 Existence of urgency outside any GDPR legal presumption and the need to derogate from the cooperation and consistency mechanisms

4.2.2.1 Summary of the position of the DE-HH SA

182. According to the DE-HH SA, the urgent need for adoption of final measures goes hand in hand with the urgency for provisional measures under Article 66(1) GDPR and the risk of serious and irreparable harm

¹⁶⁰ See EC Implementing Decision (EU) 2018/743 of 16 May 2018 on a pilot project to implement the administrative cooperation provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council by means of the Internal Market Information System C/2018/2814, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.123.01.0115.01.ENG&toc=OJ%3AL%3A2018%3A123%3ATOC.

for the rights and freedoms of data subjects without the adoption of final measures. The DE-HH SA considers that the Updated Terms lead to a more intensive use of WhatsApp's user data by Facebook IE, such as location information or message content without a transparent and reasonable legal basis. The DE-HH SA considers that Facebook IE's infringement of Articles 5(1), 6(1) and 12(1) GDPR will continue if no final measure is adopted.¹⁶¹

183. The DE-HH SA considers that the exceptional risks for the right to data protection of data subjects are imminent. WhatsApp's users were requested to consent to the Updated Terms by 15 May 2021, which makes imminent the risk of new processing of WhatsApp's user data by Facebook IE . The DE-HH SA considers that the exceptional intensity of the interference with the right to data protection of data subjects, and the exceptionally high number of data subjects using WhatsApp's services, require a derogation from the regular cooperation and consistency procedures in order to "*safeguard the status quo*".¹⁶²

184. According to the DE-HH SA, ceasing to use WhatsApp is not likely to be a serious alternative for many users, as it is the most widely used messenger service in Germany, with 58 million active users in 2019, and it is also a closed system. The DE-HH SA further considers that if WhatsApp IE's users decide to give their consent, they run the risk that their data will be used by Facebook while they cannot see the extent of this use. Once Facebook starts merging WhatsApp's user data with its own data sets, complete disentanglement of the data sets will no longer be possible.¹⁶³

185. The DE-HH SA therefore considers that it is unacceptable for data subjects to wait and see how the situation develops, since a *fait accompli* can be created by Facebook at any time after 15 May 2021. In the DE-HH SA's view, the fact that similarly worded consents have already been requested from users in the past does not remove the urgency, because these consents are currently being legally renewed, precisely in order to justify a data exchange, at least for the future. The DE-HH SA expects that Facebook products will merge even more and the data transfer between the Facebook Companies will grow¹⁶⁴, which will further increase the number of people affected.¹⁶⁵

186. Therefore, in the view of DE-HH SA, the exceptional severity of the interference with data subjects' rights and freedoms results from the number and composition of the persons affected by the processing, as well as from the quality of the interference.¹⁶⁶

¹⁶¹ DE-HH SA's, Letter to the EDPB Chair requesting a binding decision of the EDPB according to Article 66(2) GDPR, 3 June 2021, p. 5.

¹⁶² DE-HH SA Order, p. 2; DE-HH SA, Letter to the EDPB Chair requesting a binding decision of the EDPB according to Article 66(2) GDPR, 3 June 2021, pp. 3 and 9.

¹⁶³ DE-HH SA Order, section II, 1)a), pp. 9-10; DE-HH SA, letter to Facebook IE - Hearing before issuing an order in accordance with Article 58(2)(f) GDPR in conjunction with Article 66(1) GDPR, 12 April 2021, p. 11.

¹⁶⁴ The DE-HH SA cited the following references in this context: <https://www.areamobile.de/Facebook-Firma-215528/News/Messaging-bei-Facebook-und-Instagramverschmilzt-Zukuentig-auch-mit-WhatsApp-1359113/>; <https://www.netzwelt.de/news/179506-whatsapp-facebook-messenger-erste-hinweise-verschmelzung-aufgetaucht.html>; <https://about.instagram.com/blog/announcements/say-hi-to-messenger-introducing-new-messaging-features-for-instagram>

¹⁶⁵ DE-HH SA Order, section II, 1)a), pp. 9-10; DE-HH SA, letter to Facebook IE - Hearing before issuing an order in accordance with Article 58(2)(f) GDPR in conjunction with Article 66(1) GDPR, 12 April 2021, p. 11.

¹⁶⁶ DE-HH SA, letter to the EDPB Chair requesting a binding decision of the EDPB according to Article 66(2) GDPR, 3 June 2021, p. 7; as well as DE-HH SA Order of 10 May 2021, section II 1)b), p. 9; and DE-HH SA, letter to Facebook IE - Hearing before issuing an order in accordance with Article 58(2)(f) GDPR in conjunction with Article 66(1) GDPR, 12 April 2021, p. 11.

187. The DE-HH SA also refers to Facebook IE's plans to process the personal data of WhatsApp's users in the context of the WhatsApp Business API, and argues that the implementation of this processing is imminent.¹⁶⁷ The DE-HH SA stated that Facebook IE intends to use WhatsApp's user data, which it receives as a so-called 'vendor'¹⁶⁸, also for its own purposes, by offering companies the publication of personalised advertisements based on the chat messages they exchange with their customers via the WhatsApp Business API. In addition to the large amount of metadata WhatsApp IE transfers to Facebook IE, Facebook IE now also has access to message content and is thus able to create a comprehensive profile of WhatsApp's users.

188. The DE-HH SA further states that "*[e]ven though WhatsApp declares on behalf of Facebook that the messages are not automatically used for advertisements that users then see on Facebook, users of both services do not learn how extensively their data is ultimately shared by both services.*"¹⁶⁹ According to the DE-HH SA, this means that "[...] users will be able to be addressed individually and directly with messages from companies, NGOs and political parties, associations and societies on WhatsApp and Facebook".¹⁷⁰ The DE-HH SA considered that "*[t]he use of these newly gained possibilities has so far been unmanageable, neither for the persons concerned nor for supervisory authorities. The data pool created by the transmission enables granular profiling, the depth of which is probably unparalleled so far. The mere fact that Facebook receives information about which persons communicate with each other via the metadata and can link this with the information already available at Facebook represents a new, unique quality of intervention.*"¹⁷¹

189. The DE-HH SA is of the opinion that "*[t]he receipt of personal data in the context of the exchange of messages between users and companies therefore leads, in the overall view, to a considerably increased quality of intervention in data processing with unforeseeable risks.*"¹⁷²

190. The DE-HH SA also refers to data protection scandals in the recent past in which Facebook was involved, such as Cambridge Analytica¹⁷³, and considers that this shows the extent of the danger for the rights and freedoms of data subjects. It further considers this danger to be all the more concrete in view of the upcoming federal elections in Germany in September 2021, and is of the view that "[...] these elections will arouse desires to influence opinion-forming on the part of Facebook's advertisers."¹⁷⁴

¹⁶⁷ DE-Hamburg SA, Letter to the EDPB Chair requesting a binding decision of the EDPB according to Art. 66 (2) GDPR, 3 June 2021, p. 6.

¹⁶⁸ The appropriate GDPR terminology would be "processor".

¹⁶⁹ DE-HH SA Order, section II, 1)b), p. 10; DE-HH SA, letter to Facebook IE - Hearing before issuing an order in accordance with Article 58(2)(f) GDPR in conjunction with Article 66(1) GDPR, 12 April 2021, p. 11; DE-HH SA, letter to the EDPB Chair requesting an urgent binding decision of the EDPB according to Article 66(2) GDPR, 3 June 2021, p. 8.

¹⁷⁰ DE-HH SA Order, section II, 1)b), p. 10.

¹⁷¹ DE-HH SA Order, section II, 1)b), pp. 10-11.

¹⁷² DE-HH SA Order, section II, 1)b), p. 11.

¹⁷³ The DE-HH SA quoted the following references in this context: UK SA (ICO)'s findings on the Brexit referendum: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/>; EDPB Opinion 2/2019 on the use of personal data in political campaigns: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf; Opinion of the Icelandic SA on the use of social media by political parties before general elections - guidance and proposals: <https://www.personuvernd.is/information-in-english/greinar/nr/2880>.

¹⁷⁴ DE-HH SA Order, section II, 1)b), p. 11. In this context, the DE-HH SA quoted the following references: Former NATO Secretary General Anders Fogh Rasmussen on election interference: "Germany is more vulnerable than

191. The DE-HH SA states that Facebook IE and WhatsApp IE's assertion that "[n]o Alleged Processing is taking place, or will take place, as a consequence of the WhatsApp Update, in line with the present Commitments" does not influence the necessity of the DE-HH SA Order. In DE-HH SA's view, this assertion only indicates that such processing will not take place as a consequence of the Updated Terms, and that Facebook IE and WhatsApp IE do not deny that such processing is planned to take place in the near future.¹⁷⁵

192. The DE-HH SA further states that, from the considerations above, it becomes clear that Facebook IE and WhatsApp IE are of the opinion that users' consents to another (further) update of WhatsApp's user-facing information are not necessary for processing WhatsApp's users data of by Facebook IE for its own purposes listed in the DE-HH SA Order¹⁷⁶. Moreover, the DE-HH SA considers that any actual data transfer is linked to the prerequisite of accepting WhatsApp's terms of service and privacy policy.¹⁷⁷

193. Based on its analysis of WhatsApp IE's public-facing information, the DE-HH SA considers that data exchanges between WhatsApp and Facebook are currently taking place, or will take place imminently, and that it also implies the sharing of WhatsApp's user data for Facebook IE's own purposes.¹⁷⁸

4.2.2.2 Analysis of the EDPB

194. As regards the processing relating to WhatsApp Business API data, the previous version of the Updated Terms already informed WhatsApp's users that "*businesses may use another company to assist it in storing, reading and responding to your message on behalf and in support of that business*". The new version of the Privacy Policy made it clear that the other Facebook Companies can become one of those service providers. However, as the Board concluded that, at this stage, there are not enough elements allowing to establish with certainty that Facebook IE already started or will soon start

ever to disinformation", <https://www.spiegel.de/politik/deutschland/bundestagswahl-deutschland-ist-gefaehrdeter-denn-je-was-disinformation-angeht-a-f9565251-773d-47d3-9986-b1808dcabf94>; Germany is more targeted by Russian disinformation campaigns than any other country in the European Union, according to an EU investigation: <https://www.rnd.de/politik/russland-deutschland-laut-eu-im-fokus-russischer-disinformation-LF6PGVYYVKDANH346E5WA7WQG4.html>.

¹⁷⁵ Joint letter from Facebook IE and WhatsApp IE to the EDPB Chair, dated 14 May 2021, p. 1, quoted by DE-HH SA, letter to the EDPB Chair requesting a binding decision of the EDPB according to Article 66(2) GDPR, 3 June 2021, p. 5.

¹⁷⁶ In the view of Facebook IE, the DE-HH SA mistakenly assumes that, by asking users to accept updated Terms of Service as part of the update foreseen in May 2021, WhatsApp IE is seeking to obtain consent in order to be able to rely on Article 6(1)(a) GDPR for an alleged new form of processing. According to Facebook IE, the request to accept new Terms of Service as part of the update is merely a means for WhatsApp IE to obtain contractual acceptance to the latest version of its contractual terms. Facebook IE states that it is not an attempt to obtain consent to data processing pursuant to Article 6(1)(a) GDPR, and is not relied upon as such (Facebook IE's written submissions to the DE-HH SA, section 1.1 (C), pp. 2-3; and joint letter from Facebook IE and WhatsApp IE to the EDPB, 14 May 2021, p. 2). Facebook IE further states that according to its understanding, WhatsApp IE intends to achieve the following two goals with the update foreseen for May 2021: (1) to improve transparency for data subjects about how WhatsApp IE currently processes their data, specifically in light of the IE SA's comments and preliminary findings in its ongoing cross-border statutory inquiry on WhatsApp's public-facing information; and (2) to provide additional information about how messaging a business works on the WhatsApp service (Facebook IE's written submissions to the DE-HH SA, section 2, 2.15, p. 10; and joint letter from Facebook IE and WhatsApp IE to the EDPB, 14 May 2021, p. 2; as well as WhatsApp IE's letter to the IE SA, 5 February 2021, pp. 1-2).

¹⁷⁷ DE-HH SA, letter to the EDPB Chair requesting an urgent binding decision of the EDPB according to Article 66(2) GDPR, 3 June 2021, p. 6.

¹⁷⁸ DE-HH SA, letter to the EDPB Chair requesting an urgent binding decision of the EDPB according to Article 66(2) GDPR, 3 June 2021, p. 8.

processing WhatsApp' user data in the context of the WhatsApp Business API service as a controller, the EDPB cannot establish an urgency to intervene under Article 66(2) GDPR.

195. As regards the processing made for the four other purposes identified by the DE-HH SA, including safety, security and integrity, as well as product improvement, the EDPB considers that the elements contained in WhatsApp's public-facing information, on the basis of which the EDPB considers the existence of a likelihood that Facebook IE is processing WhatsApp's user data as controller, were already included in the previous version of WhatsApp's public-facing information¹⁷⁹.
196. In the view of the EDPB, the occasion of the adoption of the Updated Terms that contain similar problematic elements as in the previous version cannot, on its own, justify the urgency for the EDPB to order the LSA to adopt final measures under Article 66(2) GDPR. **The EDPB therefore considers that there is no urgency for the LSA to adopt final measures in this case.**
197. However, EDPB would like to underline the high likelihood that the processing by Facebook IE as controller for both the purpose of safety, security and integrity and the purpose of product improvement is taking place. This important matter requires swift actions to carry out a statutory investigation, in particular for verifying if, in practice, the processing made by the Facebook Companies implying 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, is currently taking place. Considering the existence of references to such processing within WhatsApp's public-facing information, and the amount of time which has elapsed since 2018, the EDPB is of the view that the IE SA needs to swiftly take action. For this reason, the EDPB, taking note of proceedings and actions already under way by the LSA to investigate matters relating to Facebook IE and WhatsApp IE, requests the LSA to carry out, as a priority matter, an 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 Article 5(1)(a) and Article 6(1) GDPR.

4.2.3 Conclusion

198. The EDPB considers that **there is no urgency for the LSA to adopt final measures.**

5 ON THE APPROPRIATE FINAL MEASURES

199. Considering the fact that **the conditions** relating to the demonstration of the existence of an infringement and urgency **are not met** (see above points 4.1.7. and 4.2.3), the EDPB concludes that it sees no reason to request the adoption of final measures against Facebook IE.

¹⁷⁹ The DE-HH SA already sent a letter to the IE SA on 3 January 2019 underlining the language showing supporting the view that Facebook IE is processing data as data controller and asking the IE SA to request Facebook IE and WhatsApp IE proof of compliance. The DE-HH SA offered to carry out a joint action.

6 URGENT BINDING DECISION

200. In light of the above and in accordance with the tasks of the EDPB under Article 70(1)(t) GDPR to issue urgent binding decisions pursuant to Article 66 GDPR, the Board issues the following binding decision in accordance with Article 66(2) GDPR:
201. As regards the existence of infringement, based on the evidence provided, there is a high likelihood that Facebook IE already processes WhatsApp's user data as a (joint) controller for the common purpose of safety, security and integrity of WhatsApp IE and the other Facebook Companies, and for the common purpose of improvement of the products of the Facebook Companies. However, the EDPB is not in a position to determine whether such processing takes place in practice.
202. There is also not sufficient information in the present procedure to establish with certainty that Facebook IE 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, and that Facebook IE already started and that it or will soon start processing WhatsApp's user data as a (joint) controller for its own purpose in relation to WhatsApp Business API.
203. The EDPB considers that it does not have sufficient information in the present procedure to conclude whether infringements are taking place.
204. On the existence of urgency, the EDPB considers that Article 61(8) GDPR is not applicable in this specific case, hence that the urgent nature of the DE-HH SA's Article 66(2) GDPR request needs to be demonstrated.
205. The EDPB considers that the occasion of the adoption of the Updated Terms that contain similar problematic elements as the previous version cannot, on its own, justify the urgency for the EDPB to order the LSA to adopt final measures under Article 66(2) GDPR. The EDPB therefore considers that there is no urgency for the LSA to adopt final measures in this case.
206. Taking this into consideration, the EDPB decides that **no final measures need to be adopted** against Facebook IE.
207. The EDPB considers that the high likelihood of infringements and the lack of information relating to the five purposes identified above justifies the decision to request the IE SA to carry out a statutory investigation, in particular for verifying if, in practice:
- the processing made by the Facebook Companies for the purposes of safety, security and integrity, as well as product improvement, implying 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 for instance by the use of unique identifiers in relation to the purpose of product improvement, are currently taking place, and what are the roles of the Facebook Companies involved;
 - Facebook IE has already started to process WhatsApp's user data as a (joint) controller for its own purposes of marketing communications and direct marketing, as well as cooperation with the other Facebook Companies, and what are the roles of the Facebook Companies involved;
 - Facebook IE has already started or will soon start to process WhatsApp's user data as a (joint) controller for its own purpose in relation to WhatsApp Business API, and what are the roles of the Facebook Companies involved, as well as the role of the businesses, in particular where businesses decide to rely on Facebook for advertisements.

- Facebook IE, when using the content of messages sent via WhatsApp to businesses, would be acting as (joint) controller.

Considering the high likelihood of infringements for the purpose of safety, security and integrity of WhatsApp IE and the other Facebook Companies, as well as for the purpose of improvement of the products of the Facebook Companies, the EDPB decides that the IE SA shall carry out, as a priority matter, an 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 Article 5(1)(a) and Article 6(1) GDPR

7 FINAL REMARKS

208. This urgent binding decision is addressed to the IE SA, the DE-HH SA and the other CSAs.
209. The IE SA shall notify this urgent binding decision to Facebook IE and WhatsApp IE without delay.
210. Once such communication is done by the IE SA, this urgent binding decision will be made public on the EDPB's website without delay after the notification to Facebook IE.
211. The EDPB considers that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Binding decision of the Board (Art. 66)



**Urgent Binding Decision 01/2023 requested by the
Norwegian SA for the ordering of final measures regarding
Meta Platforms Ireland Ltd (Art. 66(2) GDPR)**

Adopted on 27 October 2023

Table of contents

1	Summary of facts.....	4
1.1	Summary of the relevant events	4
1.2	Submission of the request to the EDPB and related events	14
2	Competence of the EDPB to adopt an urgent binding decision under Article 66(2) GDPR	15
2.1	The SA has taken provisional measures under Article 66(1) GDPR.....	15
2.2	Existence of a request pursuant to Article 66(2) GDPR coming from a SA in the EEA.....	16
2.3	Conclusion	16
3	The right to good administration	16
4	On the need to request final measures.....	17
4.1	On the existence of infringements	17
4.1.1	On the infringement of Article 6(1) GDPR.....	18
4.1.2	On the infringement of the duty to comply with decisions by supervisory authorities	42
4.2	On the existence of urgency to adopt final measures by way of derogation from the cooperation and consistency mechanisms	45
4.2.1	On the existence of urgency and the need to derogate from the cooperation and consistency mechanisms.....	46
4.2.2	On the application of a legal presumption of urgency justifying the need to derogate from the cooperation and consistency mechanisms	56
4.2.3	Conclusion as to the existence of urgency	65
5	On the appropriate final measures	65
5.1	Content of the final measures.....	65
5.1.1	Summary of the position of the NO SA	65
5.1.2	Summary of the position of Meta IE and Facebook Norway	66
5.1.3	Analysis of the EDPB	69
5.1.4	Conclusion	76
5.2	Adoption of the final measures and notification to the controller.....	76
6	Urgent Binding Decision	77
7	Final remarks	78

The European Data Protection Board

Having regard to Article 66 of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter '**GDPR**')¹,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018²,

Having regard to Articles 11, 13, 23 and 39 of the EDPB Rules of Procedure³, hereinafter the '**EDPB RoP**'.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the '**EDPB**' or the '**Board**') is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it can adopt opinions and binding decisions under different circumstances described under Articles 63 to 66 GDPR, within the consistency mechanism. The GDPR also established a cooperation mechanism, as it follows from Article 60 GDPR that the lead supervisory authority (hereinafter '**LSA**') shall cooperate with the other supervisory authorities concerned (hereinafter '**CSAs**') in an endeavour to reach consensus.

(2) Pursuant to Article 66(1) GDPR, in exceptional circumstances, where a supervisory authority ('**SA**') considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 GDPR or the procedure referred to in Article 60 GDPR, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months.

(3) In accordance with Article 66(2) GDPR, where a supervisory authority has taken a measure pursuant to Article 66(1) GDPR and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

(4) In accordance with Article 13(2) EDPB RoP, the supervisory authority requesting an urgent binding decision shall submit any relevant document. When necessary, the documents submitted by the competent supervisory authority shall be translated into English by the EDPB Secretariat. Once the Chair and the competent supervisory authority have decided that the file is complete, it is communicated via the EDPB Secretariat to the members of the Board without undue delay.

(5) Pursuant to Article 66(4) GDPR and Article 13(1) EDPB RoP, the urgent binding decision of the EDPB shall be adopted by simple majority of the members of the EDPB within two weeks following the decision by the Chair and the competent supervisory authority that the file is complete.

¹ OJ L 119, 4.5.2016, p. 1.

² References to 'Member States' made throughout this decision should be understood as references to 'EEA Member States'. References to 'EU' should be understood, where relevant, as references to 'EEA'.

³ EDPB Rules of Procedure, adopted on 25 May 2018, as last modified and adopted on 6 April 2022.

1 SUMMARY OF FACTS

1. This document contains an urgent binding decision adopted by the EDPB pursuant to Article 66(2) GDPR, following a request made by the Norwegian supervisory authority - 'Datatilsynet' (hereinafter, the '**NO SA**') within the framework of the urgency procedure under Article 66 GDPR.

1.1 Summary of the relevant events

2. On 31 December 2022, the Irish supervisory authority ('Data Protection Commission', hereinafter the '**IE SA**') issued a final decision concerning the inquiry IN-18-5-5 (hereinafter, the '**IE SA FB Decision**', related to the Facebook Service) and a final decision concerning the inquiry IN-18-5-7 (hereinafter, the '**IE SA IG Decision**', related to the Instagram Service) in which it found that Meta Platforms Ireland Ltd (hereinafter, '**Meta IE**') did not rely on a valid legal basis for processing personal data for behavioural advertising purposes⁴. These two decisions (hereinafter, collectively, the '**IE SA Decisions**') were adopted on the basis of EDPB Binding Decisions 3/2022 and 4/2022, adopted by the EDPB pursuant to Article 65(1) (a) GDPR on 5 December 2022 (hereinafter, the '**EDPB Binding Decisions**')⁵.
3. Each of the IE SA Decisions concluded that Meta IE was not entitled to rely on Article 6(1)(b) GDPR to carry out processing of personal data for the purpose of behavioural advertising in the context of the Facebook Terms of Service / Instagram Terms of Use⁶ and included an order, addressed to Meta IE, to bring its processing of personal data for behavioural advertising purposes into compliance with Article 6(1) GDPR within three months⁷.
4. On 5 April 2023, the IE SA shared with the CSAs⁸, using the Internal Market Information system (hereinafter, '**IMI**')⁹, Meta IE's compliance reports regarding the Facebook Service (IN-18-5-5) and the Instagram Service (IN-18-5-7) (hereinafter collectively, the '**Meta IE Compliance Reports**' or the '**Compliance Reports**')¹⁰ and supporting material that Meta IE submitted to the IE SA on 3 April 2023

⁴ Decision of the Irish Data Protection Commission of 31 December 2022, DPC Inquiry Reference: IN-18-5-5, concerning a complaint directed against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Facebook Service (the '**IE SA FB Decision**'); Decision of the Irish Data Protection Commission of 31 December 2022, DPC Inquiry Reference: IN-18-5-7, concerning a complaint directed against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Instagram Service (the '**IE SA IG Decision**').

⁵ EDPB Binding Decision 3/2022, adopted on 05 December 2022 (hereinafter '**EDPB Binding Decision 3/2022**'); EDPB Binding Decision 4/2022 adopted on 05 December 2022 (hereinafter '**EDPB Binding Decision 4/2022**'). In each of these binding decisions the EDPB instructed the IE SA to alter its Finding 2 of its Draft Decision, which concluded that Meta IE may rely on Art. 6(1)(b) GDPR in the context of its offering of the Facebook Terms of Service or the Instagram Terms of Use and to include an infringement of Art. 6(1) GDPR based on the shortcomings that the EDPB has identified in the EDPB Binding Decisions. The reasoning of the EDPB is available in paragraphs 94-133 and 484 of EDPB Binding Decision 3/2022 and in paragraphs 97-137 and 451 of EDPB Binding Decision 4/2022.

⁶ IE SA FB Decision, Finding 2, p. 49; IE SA IG Decision, Finding 2, p. 49.

⁷ IE SA FB Decision, paragraphs 8.8, 10.44; IE SA IG Decision, paragraphs 212, 417. The deadline for compliance with the orders in the IE SA Decisions fell on 5 April 2023.

⁸ In the cases leading to the adoption of the IE SA Decisions, all EEA SAs were CSAs pursuant to the GDPR (IE SA FB Decision, Schedule 1, paragraph 1.10; IE SA IG Decision, Appendix 1 - Schedule 1, paragraph 6).

⁹ More specifically, the IE SA shared on 5 April 2023 the Meta IE Compliance Reports via two IMI workflows, one for the IE SA FB Decision and one for the IE SA IG Decision respectively (hereinafter, collectively, the '**IE SA IMI Informal Consultations**' or the '**IMI Informal Consultations**').

¹⁰ Meta IE's Compliance Report regarding the Facebook Service (IN-18-5-5) of 3 April 2023 (hereinafter, '**Meta IE Compliance Report on IE SA FB Decision**'), paragraphs 2.1 and 2.3 and Meta IE's Compliance Report

with the aim of showing compliance with the IE SA Decisions. In its Compliance Reports, Meta IE indicated that it changed its legal basis for the majority¹¹ of its processing of personal data for behavioural advertising purposes from Article 6(1)(b) GDPR to Article 6(1)(f) GDPR as of 5 April 2023, which was the deadline for compliance with the IE SA Decisions¹². Specifically for reliance on Article 6(1)(f) GDPR, Meta IE provided legitimate interests assessments as supporting materials¹³ (hereinafter collectively, the '**Meta IE Legitimate Interests Assessments**'). Without providing its own analysis on the Compliance Reports, the IE SA invited all the CSAs to assess the extent to which the measures implemented by Meta IE achieved compliance with the orders in the IE SA Decisions and welcomed feedback from the CSAs by 5 May 2023. The deadline was later on extended to 15 May 2023¹⁴.

5. On the same day, the NO SA emailed the IE SA in respect of Meta IE's change of legal basis to legitimate interest, expressing strong doubts as to whether this legal basis could be validly relied on and asking for the IE SA's preliminary view on this.
6. On 6 April 2023, upon request of the IE SA, the EDPB Secretariat circulated a message from the IE SA to the members of the Enforcement expert subgroup within the EDPB. Such message aimed to attract all CSAs' attention to the IE SA IMI Informal Consultations circulated by the IE SA via IMI¹⁵. On the same day, the IE SA replied to the NO SA's email of 5 April 2023, pointing to the message from the IE SA to the CSAs circulated by the EDPB Secretariat.
7. On 13 April 2023, the IE SA shared with the CSAs via IMI two further letters from Meta IE (one on the IE SA FB Decision and one on the IE SA IG Decision) dated 12 April 2023, providing further information on its compliance efforts in relation to the IE SA Decisions.
8. On 14 April 2023, the NO SA responded negatively to a meeting request from Meta IE dated 28 March 2023, pointing out that the case is handled by the IE SA as the LSA.
9. Some CSAs asked for clarifications on the procedure being followed, for example on the reasons why the IE SA did not at that point share its assessment of Meta IE's compliance with the orders in the IE SA Decisions. The IE SA clarified, first, that the assessment of compliance with the orders in the IE SA Decisions would be carried out on a joint basis, more specifically by way of an assessment carried out by the CSAs at the same time as the LSA, and that this sequencing of the process was aimed to ensure a timely and consistent approach, in line with the deadline for compliance determined by the EDPB,

regarding the Instagram Service (IN-18-5-7) of 3 April 2023 (hereinafter, '**Meta IE Compliance Report on IE SA IG Decision**'), paragraphs 2.1 and 2.3.

¹¹ According to the Compliance Reports, Meta IE continued to process limited categories of non-behavioural information to show advertising on Facebook or Instagram based on Art. 6 (1) (b) GDPR. See Meta IE Compliance Report on IE SA FB Decision, paragraphs 3.1.3 and 5.8.2, and Meta IE Compliance Report on IE SA IG Decision, paragraphs 3.1.3 and 5.8.2.

¹² Meta IE Compliance Report on IE SA FB Decision, paragraph 2.1; Meta IE Compliance Report on IE SA IG Decision, paragraph 2.1.

¹³ Meta IE's Legitimate Interests Assessments Behavioural Advertising Processing of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision.

¹⁴ Following requests from two of the CSAs, the deadline to share feedback was extended until 15 May 2023. In fact, the IE SA waited for a few more days, giving the opportunity to further CSAs to share their views.

¹⁵ In the same message, the IE SA also specified: 'As you will also recall, IE SA confirmed, during the Article 65 [GDPR] discussions, that any assessment of compliance with the orders made [in the IE SA Decisions] would be carried out on a joint basis, the same as in previous cases, whereby the IE SA together with all CSAs would jointly assess the extent to which any action taken has achieved compliance with the terms of the order'.

formulated on the basis that urgent action was required to be taken by Meta IE to address the infringement¹⁶. The IE SA also clarified that it would not issue a new draft decision¹⁷.

10. Several CSAs provided their feedback on the way in which Meta IE complied with the IE SA Decisions.

- The Österreichische Datenschutzbehörde (Austrian supervisory authority - hereinafter, the '**AT SA**') shared its views that processing operations in connection with behavioural advertising could not be based on Article 6(1) (f) GDPR¹⁸.
- The Integritetsskyddsmyndigheten (Swedish supervisory authority - hereinafter, the '**SE SA**') stressed the importance of adhering to any applicable EDPB guidelines¹⁹.
- The Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (hereinafter, the '**DE Hamburg SA**') shared its views stating that 'at this stage, consent would be the only possible legal basis to comply with' the orders in the IE SA Decisions, and expressing concerns regarding the indications that sensitive data are processed without consent and regarding the processing activities for which Meta IE continued to rely upon Article 6(1)(b) GDPR²⁰.
- The Autoriteit Persoonsgegevens (Dutch supervisory authority - hereinafter the '**NL SA**') shared its views that 'the interests listed by [Meta IE] in the/its Legitimate Interest Assessment cannot be considered as "legitimate interests" in the sense of Article 6(1) (f) GDPR', the processing of personal data is not 'necessary' for the purpose of the declared interests, and the 'fundamental rights and freedoms of the data subject override the interest of [Meta IE] and the third parties involved'²¹.
- The NO SA transmitted on 5 May 2023 a formal mutual assistance request under Article 61 (1) GDPR²² (hereinafter, the '**NO SA Mutual Assistance Request**') to the LSA using the dedicated

¹⁶ These clarifications were made by the IE SA on 26 April 2023 as a reply to a question of the FR SA of 25 April 2023 made in the IE SA IMI Informal Consultations.

¹⁷ The SE SA asked for clarification on the procedure being followed on 4 May 2023 via the IMI Informal Consultations. The IE SA replied on 5 May 2023.

¹⁸ These views were shared as a reply to the IE SA IMI informal consultation concerning only the IE SA FB Decision (Comment of the AT SA of 18 April 2023), see footnote 9. The AT SA also indicated that a balancing test was also difficult because the term 'Behavioural Advertising Processing' was not defined in the Privacy Policy and what this actually entailed was not entirely clear. The AT SA also made reference to the reasoning in its relevant and reasoned objection to the IE SA's draft decision in the procedure leading to the adoption of the IE SA FB Decision.

¹⁹ Comment of the SE SA of 4 May 2023 as a reply to the IE SA IMI Informal Consultations, see footnote 9.

²⁰ Comment of the DE Hamburg SA of 4 May 2023 as a reply to the IE SA IMI Informal Consultations, see footnote 9. In its comments, the DE Hamburg SA stated that there 'are strong indications that sensitive data stemming from different sources are processed without consent against the Art. 9 (1) GDPR' and that 'consent [is] the only possible legal basis for that kind of processing' and made further remarks on this issue. The DE Hamburg SA also stated that the 'processing described or indicated in the updated Terms of Use and [Meta IE] Privacy Notice cannot be based on Art. 6 (1) (b) GDPR'.

²¹ Comment of the NL SA of 4 May 2023, paragraph 3 - attached as a reply to the IE SA IMI Informal Consultations, see footnote 9. The NL SA, in its comments, also 'urgently asks the [IE SA] to swiftly undertake adequate actions in order to cease the continuous illegality of the invasive processing of personal data of millions of users' (paragraph 4). In addition to providing detailed views on the applicability of Art. 6(1)(f) GDPR (paragraphs 8-63), the NL SA also stressed its concerns about the processing of special categories of data and about the compatibility of the processing of the amount of data at stake with the principles of data minimisation and purpose limitation (paragraphs 6-7).

²² Comment of the NO SA of 5 May 2023 as a reply to the IE SA IMI Informal Consultations (see footnote 9), attaching a copy of the NO SA Mutual Assistance Request introduced on 5 May 2023.

IMI flow²³. The NO SA requested the IE SA to (1) issue a temporary ban on Meta IE's processing of personal data for behavioural advertising purposes based on Article 6(1)(f) GDPR and (2) share a timeline with the NO SA and the CSAs specifying how the IE SA will ensure in an expedient manner that Meta IE complies with Article 6(1) GDPR.

- The Agencia Española de Protección de Datos (Spanish supervisory authority - hereinafter the '**ES SA**') shared its views stating that 'the submitted Legitimate Interest Assessment does not demonstrate that the processing carried out by [Meta IE] with the purpose of behavioural advertisement be based on Article 6(1)(f) GDPR since it does not meet the requirements of this Article'²⁴.
- The Tietosuojavaltuutetun toimisto (Finnish supervisory authority - hereinafter the '**FI SA**') shared its views on 15 May 2023 that 'based on the information available, it does not seem that [Meta IE] would have brought all its processing activities into compliance with the GDPR and would meet the requirements of the GDPR'²⁵.
- In addition, the Garante per la protezione dei dati personali (Italian supervisory authority - hereinafter, the '**IT SA**') shared its views on 23 May 2023 saying that '[Meta IE's] proposal is not such as to adequately implement the order to bring the processing into compliance insofar as it misclassifies part of the user-related information and thereby applies the legal basis of

²³ The formal NO SA Mutual Assistance Request contained two requests labelled as follows: '*Pursuant to Art. 61(1) GDPR, the following requests are made: i. We kindly request that the IE SA issues a temporary ban on [Meta IE]'s processing of personal data for behavioural advertising purposes on Facebook and Instagram based on Art. 6(1)(f) GDPR, in accordance with Art. 58(2)(f) GDPR. The ban should last until the lead and concerned supervisory authorities are satisfied that [Meta IE] has provided adequate and sufficient commitments to ensure compliance with Art. 6(1) GDPR and Art. 21 GDPR, in line with Art. 31 GDPR. This will give us the opportunity to further engage with [Meta IE] and make sure that it commits to fully respect its obligations under the GDPR, while preventing any further risks for data subjects stemming from [Meta IE]'s non-compliant behavioural advertising practices. Please note that in our view, behavioural advertising includes any activities where advertising is targeted on the basis of a data subject's behaviour or movements, including advertising based on perceived location'. ii. 'We kindly request that the IE SA shares a timeline specifying how it will ensure in an expedient manner that [Meta IE] complies with Art. 6(1) GDPR. We should be grateful if the IE SA, by 5 June 2023, would share the timeline and confirm that a temporary ban will be issued. If the IE SA is not in a position to comply with our request regarding [Meta IE], we may need to consider our options in relation to the adoption of provisional measures in Norway pursuant to Art. 66 GDPR. We hope that this will not be necessary and look forward to cooperating further with the IE SA within the framework of the cooperation mechanisms set out in Chapter VII GDPR'.*

²⁴ These views were shared as a reply in the IE SA IMI informal consultation concerning only the IE SA IG Decision (Comment of the ES SA of 12 May 2023). More specifically, the ES SA argued that the interests listed by Meta IE are 'purely economic or commercial interests' of Meta IE or third parties, and that in respect of the condition of necessity of the processing 'the direct link between the processing and the legitimate interest should be established and prove that there are no less intrusive alternatives for the data subjects that could serve the interest equally effectively' (p. 4). The ES SA also noted some shortcomings in the balancing test carried out by Meta IE (Comment of the ES SA of 12 May 2023, p. 5).

²⁵ Comment of the FI SA of 15 May 2023 as a reply to the IE SA IMI Informal Consultations (see footnote 9). More specifically, the FI SA expressed doubts about legitimate interest being the most suitable legal basis in the case at hand and argued that the Legitimate Interests Assessment carried out by Meta IE 'seems to be rather one-sided and superficial and fails to convince why the interests of [Meta IE] or third parties should override the interests and fundamental rights of the data subjects' (Comment of the FI SA of 15 May 2023, p. 2) and 'fails to take duly into consideration the volume of the processing and the high number of users of the said services' (Comment of the FI SA of 15 May 2023, p. 2-3). The FI SA also noted that certain categories of personal data seem to still be unlawfully collected for behavioural advertising purposes under Art. 6(1)(b) GDPR (Comment of the FI SA of 15 May 2023, p. 2).

contractual performance under Article 6(1)(b) GDPR to the serving of ads which, actually, are behavioural in nature²⁶; the IT SA also highlighted some concerns concerning the switch to legitimate interest for the other processing activities for behavioural advertising purposes²⁷.

11. The IE SA shared with Meta IE the feedback received from the CSAs and invited Meta IE to provide submissions on these views by 2 June 2023²⁸.
12. On 30 May 2023, the NL SA sent the IE SA a request for mutual assistance under Article 61 GDPR (hereinafter, the '**NL SA Mutual Assistance Request**') asking the IE SA to provide its conclusion as to whether Meta IE could rely on Article 6 (1) (f) GDPR, its conclusion as to whether Meta IE complies with the IE SA Decisions and as to a timeframe, which appropriate and expedient action will be taken to ensure that Meta IE acts in compliance with Article 6 GDPR²⁹.
13. On 31 May 2023, the IE SA provided an update to all CSAs via the IE SA IMI Informal Consultations (hereinafter, the '**IE SA Update to CSAs of 31 May 2023**', informing them about the NL SA Mutual Assistance Request and highlighting that it will be in a position to complete its own assessment of the Meta IE Compliance Reports and share its assessment with the NO SA and NL SA (who lodged Article 61 GDPR requests) and all other CSAs by the end of June 2023. In particular, the IE SA indicated that they had 'received all of the assessments from CSAs' and 'forwarded them to [Meta IE] for it to consider the views expressed and to detail any changes that it proposes to implement on foot of the CSA assessments'. Furthermore, the IE SA stated that it will 'complete its own assessment of [Meta IE]'s compliance reports' after receiving Meta IE's response. The IE SA also stated 'it will be in a position to complete its own assessment of [Meta IE]'s compliance reports and to share its assessment with the Norwegian and Dutch supervisory authorities (both of which have lodged Article 61 requests for mutual assistance) and with all other CSAs by the end of June 2023'.
14. Also, on 31 May 2023, Meta IE sent a letter to the IE SA providing its views and comments on the process that was being followed by the IE SA and asking for an extension of its deadline to provide a reply. In this context, it also provided some comments to the IE SA on the CSAs' feedback and some preliminary comments on the requests for urgent enforcement action from some CSAs.

²⁶ Comment of the IT SA of 23 May 2023 as a reply to the IE SA IMI Informal Consultations (see footnote 9). As indicated in footnote 11, Meta IE indicated in its Compliance Reports the fact that it continued to process some data under Art. 6(1)(b) GDPR. The IT SA argued in this respect that '[Meta IE]'s distinction between non-behavioural and behavioural advertising can be said to be artificial and based merely on language' (Comment of the IT SA of 23 May 2023, p. 1)

²⁷ Comment of the IT SA of 23 May 2023 as a reply to the IE SA IMI Informal Consultations (see footnote 9). More specifically, according to the IT SA, 'it is as if the controller was shifting the burden of proof regarding legitimate interest as the legal basis of processing on the data subjects – who conversely should be called into play as key actors in the two subsequent steps of the legitimate interest test, i.e. when assessing the necessity of the processing and performing the required balancing exercise' (Comment of the IT SA of 23 May 2023, p. 2). The IT SA also underlined that 'the processing operations underpinning the use of Online Behavioural Advertising should more appropriately be grounded in consent as a legal basis within the meaning of Art. 6(1) (a) GDPR' (p.3).

²⁸ On 12 May 2023 and 16 May 2023, the IE SA sent two letters to Meta IE, providing Meta IE with the first replies received from CSAs informing Meta IE that some CSAs requested an extension of time to provide a response. On 25 May 2023, the IE SA transmitted to Meta IE the latest comments from CSAs with respect to the way in which Meta IE complied with the IE SA Decisions. The IE SA invited Meta IE to provide submissions by 2 June COB. On 26 May 2023, the IE SA shared an update with all CSAs, informing them that their responses were forwarded to Meta IE, whose response was awaited by 2 June 2023.

²⁹ The IE SA provided a reply on 31 May 2023. On the same day, the IE SA provided an update to CSAs in the IMI Informal Consultations, described in the following paragraph.

15. On 2 June 2023, the IE SA provided a reply to the NO SA Mutual Assistance Request. In the notification form used, the IE SA stated that it could not comply with the request (by checking a pre-code text box), and invited the NO SA to look at the ‘detailed response uploaded by the [IE SA]’ in the IE SA IMI Informal Consultations (see above, paragraph 13).
16. On 9 June 2023, the NO SA further replied to the IE SA, via the IE SA IMI flow relating to the NO SA Mutual Assistance Request, asking whether the IE SA could ‘share their preliminary thoughts or non-bindingly indicate whether [it] may potentially be inclined to follow [the NO SA Mutual Assistance Request]’. In the same message the NO SA indicated that it would in any case await the IE SA’s response towards the end of June.
17. On 13 June 2023, the IE SA informed all CSAs via the IE SA IMI Informal Consultations that it would await the judgment of the Court of Justice of the European Union in Case C-252/21 (*Meta Platforms Inc. v Bundeskartellamt*) (hereinafter, the ‘**CJEU Bundeskartellamt Judgment**’) before sharing its assessment of the Meta IE Compliance Reports³⁰. The IE SA, noting the NO SA Mutual Assistance Request and the NL SA Mutual Assistance Request, indicated their intention to finalise their assessment as soon as possible after the CJEU Bundeskartellamt Judgment expected on 4 July 2023.
18. On 14 June 2023, the IE SA sent a letter to Meta IE replying to its letter of 31 May 2023. The IE SA explained its intention to wait for the CJEU Bundeskartellamt Judgment before circulating its provisional assessment of the steps taken by Meta IE in purported compliance with the orders in the IE SA Decisions, as well as the expected next steps leading to the issuance of the final outcome of the assessment of compliance. In the same letter, the IE SA informed Meta IE that it no longer required it to make submissions in reply to the CSAs’ initial observations.
19. On 21 June 2023, Meta IE shared with the IE SA its views on the concerns raised by some of the CSAs and regarding potential urgent proceedings. On 23 June 2023, the IE SA shared via the IMI Informal Consultations the communication received from Meta IE on 21 June 2023. The IE SA stated that Meta IE specified that this communication is without prejudice to Meta IE’s position that it brought its processing into compliance with the orders in the IE SA Decisions.
20. On 30 June 2023, Meta IE shared by letter additional information with the IE SA regarding the IE SA’s proposed compliance assessment. In this letter, Meta IE outlined its views on the next steps envisaged by the IE SA and provided information and arguments on what it considered to be misunderstandings underpinning the views provided by the CSAs on the Meta IE Compliance Reports³¹.
21. On 4 July 2023, the Court of Justice of the European Union delivered the CJEU Bundeskartellamt Judgment³². On 6 July 2023, the IE SA indicated to all the CSAs via the IE SA IMI Informal Consultations

³⁰ The CJEU had just announced that it would deliver the judgment before the IE SA gave this update to the CSAs.

³¹ Letter from Meta IE to the IE SA of 30 June 2023. Meta IE’s comments on the next steps envisaged by the IE SA are available in paragraphs 1-3 of this letter. Meta IE also provided clarifications, information and arguments on what it considered to be misunderstandings underpinning the views provided by the CSAs on the Meta IE Compliance Reports in paragraph 7. By way of example, Meta IE stated that it ‘does not engage in a “balancing” exercise on receipt of a valid objection’, that the IE SA Decisions only apply to processing for behavioural advertising purposes (and not to processing of non-behavioural information for advertising purposes), and that the assessment of ‘Behavioural Advertising Processing’ only concerns data relating to activity on Facebook and Instagram (on-platform data). Meta IE also clarified that it relies on Art. 6(1)(a) GDPR to process information provided to Meta IE by third party advertising partners (‘off-platform data’) for the purposes of showing personalised advertisements.

³² Judgment of the Court of Justice of the European Union of 4 July 2023, *Meta Platforms Inc. v Bundeskartellamt*, C-252/21, EU:C:2023:537.

that it was considering such judgment in the context of finalising its provisional assessment of the steps taken by Meta IE in purported compliance with the IE SA Decisions³³.

22. On 11 July 2023, the IE SA issued a provisional position paper ('IE SA Provisional Position Paper') in which it preliminarily concluded that Meta IE had not complied with the orders in the IE SA Decisions, and shared it with the CSAs alongside a letter dated 30 June 2023 received from Meta IE³⁴. The IE SA invited the CSAs to share their views on the IE SA Provisional Position Paper by 21 July 2023³⁵.
23. Between 20 July 2023 and 21 July 2023, two CSAs shared their views on the IE SA Provisional Position Paper via the IE SA IMI Informal Consultations³⁶. The IE SA shared these CSAs' views with Meta IE on 21 July 2023.
24. On 14 July 2023, the NO SA imposed a temporary ban on Meta IE and Facebook Norway AS ('Facebook Norway') regarding the processing of personal data of data subjects in Norway for behavioural advertising for which Meta IE relies on Article 6(1)(b) GDPR or Article 6(1)(f) GDPR (the 'NO SA Order' or the 'Provisional Measures'). On the same day, the NO SA informed by email the IE SA of the Provisional Measures being taken on the basis of Article 66(1) GDPR. On 7 August 2023, the NO SA rejected Meta IE's and Facebook Norway's request for deferred implementation of the NO SA Order.
25. On 20 July 2023, the IE SA shared an update to the CSAs via the IE SA IMI Informal Consultations, informing the CSAs of its views on the NO SA Order. It also stated that it did not mean to refuse to comply with the NO SA Mutual Assistance Request as this was a result of '*incorrectly (and inadvertently)* checking a box and that, in its view, its communication to the NO SA of 2 June 2023 was referring to two documents shared with all CSAs on 31 May 2023³⁷, which '*directed to the subject matter of the NO SA [Mutual Assistance Request]*' and were '*clearly engaging with the substance of the NO SA [Mutual Assistance Request] [...]*'.
26. On 24 July 2023, the NO SA answered to questions from a politician in the Irish national parliament on the NO SA Mutual Assistance Request. In its reply, the NO SA describes the reply provided by the IE SA to the NO SA Mutual Assistance Request and explains the reasons behind the issuance of the Provisional Measures, expressing its concerns that 'while it is very clear that [Meta IE] does not comply with the GDPR, failing to take specific and resolute enforcement action would lead to a cat-and-mouse game whereby [Meta IE] is able to evade compliance indefinitely' and that 'simply stating that [Meta IE] does not comply with the GDPR [...] without imposing any specific order spelling out what [Meta IE] must potentially do to comply with the law and by which date, will allow [Meta IE] to further delay compliance'.

³³ In the same communication, the IE SA also indicated they expected to be in a position to circulate their provisional assessment the following week, and that they would then give the CSAs a period of ten days to respond. While the NO SA and the IE SA indicated that this update occurred on 5 July 2023, according to the IMI reports relating to the IE SA IMI Informal Consultations, this update seems to have been sent on 6 July 2023.

³⁴ This letter was already mentioned above in paragraph 20.

This update was shared by the IE SA via the IE SA IMI Informal Consultations. Together with the IE SA Provisional Position Paper and the Letter from Meta IE to the IE SA of 30 June 2023, the IE SA also shared again the Meta IE Compliance Reports (already shared on 5 April 2023 with the CSAs).

³⁵ In the same communication, the IE SA also indicated that it would then provide the CSAs' views on the IE SA Provisional Position Paper to Meta IE inviting it to make its submissions by 4 August 2023.

³⁶ The NL SA shared its views via a document attached on 20 July 2023 and the DE Hamburg SA via a document attached on 21 July 2023.

³⁷ See paragraph 13 above.

27. On 27 July 2023, Meta IE sent a letter to the IE SA stating that it intends to ground its processing for behavioural advertising purposes³⁸ on consent (Article 6(1)(a) GDPR) (by way of “**Meta IE’s Consent Proposal**”**Meta IE’s Consent Proposal**)

³⁹. The IE SA

shared this letter with the CSAs via the IE SA IMI Informal Consultations.

28. On the same day, Meta IE sent a letter to the NO SA, making reference to the letter sent to the IE SA and requesting the NO SA to lift the Provisional Measures in light of Meta IE’s commitments to the LSA to ensure compliance by way of relying upon consent.
29. On 1 August 2023, the IE SA replied to Meta IE taking note of Meta IE’s intention to implement the necessary measures to enable it to rely on Article 6(1)(a) GDPR
- ⁴⁰.
30. Meanwhile, on 1 August 2023, Meta IE and Facebook Norway lodged a complaint with the NO SA requesting that it lifts the NO SA Order. On 3 August 2023, the NO SA rejected this complaint and on the following day the NO SA sent a letter to Meta IE and Facebook Norway requesting confirmation as to whether the NO SA Order would be complied with.
31. On 4 August 2023, Meta IE provided its response to the IE SA Provisional Position Paper. On the same date, Meta IE and Facebook Norway replied to the NO SA that they have, in their view, complied with the NO SA Order, and requested the Oslo District Court to grant a preliminary injunction against the NO SA Order.
32. On 7 August 2023, the NO SA decided to impose a coercive fine on Meta IE and Facebook Norway for the non-compliance with the NO SA Order. On 14 August 2023, Meta IE requested the deferred implementation of the coercive fine imposed on Meta IE and Facebook Norway, at least until the Oslo District Court has ruled on Meta IE’s and Facebook Norway’s applications for a preliminary injunction. On 25 August 2023, the NO SA rejected Meta IE’s and Facebook Norway’s request for deferred implementation of the coercive fine.
33. On 8 August 2023, Meta IE and Facebook Norway sent a letter to the Ministry of Local Government and Regional Development of Norway, asking it to consider Meta IE’s and Facebook Norway’s complaints against the NO SA Order submitted to the NO SA on 1 August 2023⁴¹. The Ministry of Local

³⁸

³⁹

⁴⁰ This letter was shared by the IE SA with the CSAs via the IE SA IMI Informal Consultations. The IE SA also highlighted that all the correspondence from Meta IE should be treated as confidential.

⁴¹ Meta IE sustained that the Ministry should have declared the complaint valid and the decision should have been repealed, indicating that ‘the audit did not give [Meta IE] necessary notice of its proposed actions and did not give [Meta IE] the necessary opportunity to be heard’. In addition, Facebook Norway was of the opinion that the NO SA wrongfully indicated Facebook Norway as an addressee of the decision.

Government and Regional Development of Norway responded on 10 August 2023, refusing to accommodate the request and indicating that it did not have the authority to handle complaints against the NO SA Order.

34. On 10 August 2023, Meta IE sent a letter to the IE SA [REDACTED]

[REDACTED] highlighted its concerns arising from the Article 66 GDPR proceedings arising from the Provisional Measures and running in parallel to the process led by the IE SA.

35. The IE SA responded on 11 August 2023. In its letter, the IE SA [REDACTED]

[REDACTED] highlighted that it considered it is not for it to second-guess the decision of the NO SA to trigger the application of the urgency procedure and that the Article 66 GDPR procedure would take its own course.

36. The proceedings concerning the request for preliminary injunction lodged with the Oslo District Court further developed and the parties submitted written pleadings⁴².

37. [REDACTED]

⁴³.

38. On 18 August 2023, the IE SA shared with all CSAs its final position paper ('IE SA Final Position Paper'), in which the IE SA concluded that Meta IE failed to demonstrate compliance with the orders in the IE SA Decisions⁴⁴. The IE SA also indicated its view that in light of the Meta IE's Consent Proposal, it is fair

⁴² On 10 August 2023 and 11 August 2023, respectively, Meta IE and Facebook Norway and the NO SA submitted their written pleadings to the Oslo District Court. Meta IE requested provisional injunctions to avoid damage following an alleged invalid administrative decision and Facebook Norway claimed that the NO SA's justification was inadequate. The NO SA responded to the request for a preliminary injunction claiming, *inter alia*, that there was no case processing error that may have affected the content of the decision, the conditions for urgent measures for adopting its decision were met, the decision did not violate Article 84 GDPR (proportionality) and that an injunction by the Oslo District Court would have been in a manifest disparity with the damages or inconveniences Norway would have been inflicted. Meta IE then submitted further written pleadings to the Oslo District Court on 14 August 2023. On 15 August 2023, Meta IE and Facebook Norway complained against the NO SA about the NO SA's rejection of their complaint. Meta IE and Facebook Norway reiterate that the appeal before the Ministry should be admissible and that they have the right to appeal the decision of the Ministry (contrary to the Ministry's declaration) according to administrative law. On 16 August 2023, the NO SA submitted further written pleadings to the Oslo District Court, while Meta IE and Facebook Norway submitted their additional written pleadings on 18 August 2023.

⁴³ [REDACTED]

⁴⁴ Together with the IE SA Final Position Paper, the IE SA shared with the CSAs the same supporting materials as shared together with the IE SA Provisional Position Paper. See above paragraph 22.

Also, on 17 August 2023, the IE SA provided an update to all CSAs via the IE SA IMI Informal Consultations, informing them mainly of the fact that the copies of the relevant communications to which the IE SA was party were transmitted to the NO SA and Meta IE to ensure that both the NO SA and Meta IE were in a position to put the full suite of communications before the Oslo District Court.

- and reasonable to give Meta IE an opportunity to demonstrate that it can rely on consent as its lawful basis rather than engaging in enforcement measures⁴⁵.
39. On 25 August 2023, Meta IE and Facebook Norway submitted, each, to the NO SA their comments on the NO SA's intended request for an urgent binding decision from the EDPB pursuant to Article 66 (2) GDPR, which was specified in the NO SA Order.
 40. On 28 August 2023, Meta IE and Facebook Norway complained against the NO SA regarding the coercive fine it had imposed. Meta IE and Facebook Norway asked the NO SA to revoke the enforcement decision or, at least, to lower the amount.
 41. On 6 September 2023, the Oslo District Court decided not to grant the petitions from Meta IE and Facebook Norway for a preliminary injunction against the NO SA Order.

42.

⁴⁶.

43.

⁴⁷.

44. On 21 September 2023, the NO SA sent a letter to the IE SA outlining their views on the current state of play. More specifically, the NO SA stated that it considered there is still an urgent need for a ban of the unlawful processing of personal data carried out by Meta IE despite the Meta IE's Consent Proposal⁴⁸, and that such a ban would represent an incentive for Meta IE to swiftly bring processing into compliance⁴⁹. Thus, the NO SA asked the IE SA to reconsider their position, outlined in the IE SA Final Position Paper that enforcement

⁴⁵ IE SA Final Position Paper, paragraph 9.2.

⁴⁶

⁴⁷

⁴⁸ Letter of the NO SA to the IE SA of 21 September 2023, p. 2.

⁴⁹ Letter of the NO SA to the IE SA of 21 September 2023, p. 3.

measures are not necessary at this point in time⁵⁰. The letter also mentioned that the NO SA requested submissions from Meta IE about its intention to ask the EDPB for an urgent binding decision, but may consider not making such request should the IE SA decide to adopt enforcement measures⁵¹.

45. On 26 September 2023, Meta IE and Facebook Norway made submissions in relation to the request of the NO SA for an urgent binding decision of the EDPB and the NO SA lodged its request to the EDPB on IMI. Further details on this are available below⁵².
46. On 27 September 2023, the IE SA replied to the letter of the NO SA of 21 September 2023, outlining its views on the NO SA's position and course of action. More specifically, the IE SA recalled that the EDPB explicitly declined to instruct the IE SA to impose a temporary ban in the EDPB Binding Decisions and explained that each of the IE SA Decisions 'made provision for enforcement measures, namely, the orders for compliance, under which [Meta IE]'s proposals for the adoption of one or more alternative legal bases for the [processing operations at stake] would be assessed, and ruled on, on their respective merits'⁵³. The IE SA also expressed the view that 'it is inaccurate to suggest that the [IE SA] could impose an immediate ban on processing, whilst continuing to progress its assessment of [Meta IE]'s proposed consent-based model, in conjunction with its CSA colleagues'⁵⁴.
47. On 11 October 2023, the NO SA replied to the letter of the IE SA of 27 September 2023. In this letter, the NO SA expressed its concern that despite the LSA and CSAs 'agreeing that [Meta IE] cannot base processing of personal data for behavioural advertising on Article 6(1)(b) GDPR or Article 6(1)(f) GDPR, [Meta IE] continues to violate Article 6(1) GDPR and the [IE SA Decisions], and such violation continues to be tolerated'⁵⁵. The NO SA reiterated its view that 'corrective measures can and should be imposed on [Meta IE] as soon as possible to stop [Meta IE]'s current illegal processing activities'⁵⁶.
48. The IE SA further replied on 13 October 2023. In its letter, the IE SA argued that the request of the NO SA to the EDPB amounts, in substance, to a demand for enforcement action against the IE SA for its (alleged) failure to implement the IE SA Decisions and to an attempt to use the Article 66 GDPR procedure as a means to procure an order from the EDPB to compel the IE SA to impose an EEA-wide ban on Meta IE's processing of personal data for behavioural advertising purposes⁵⁷. The IE SA also expressed its view that it did put in place an enforcement procedure following the IE SA Decisions, consistent with the EDPB Binding Decisions⁵⁸.
49. On 16 October 2023, Meta IE and Facebook Norway initiated legal proceedings before the Oslo District Court to demand the invalidation of the NO SA Order.

1.2 Submission of the request to the EDPB and related events

⁵⁰ Letter of the NO SA to the IE SA of 21 September 2023, p. 3.

⁵¹ Letter of the NO SA to the IE SA of 21 September 2023, p. 3.

⁵² See paragraph 67 below.

⁵³ Letter of the IE SA to the NO SA of 27 September 2023, p. 3.

⁵⁴ Letter of the IE SA to the NO SA of 27 September 2023, p. 4.

⁵⁵ Letter of the NO SA to the IE SA of 11 October 2023, p. 1.

⁵⁶ Letter of the NO SA to the IE SA of 11 October 2023, p. 1.

⁵⁷ Letter of the IE SA to the NO SA of 13 October 2023, p. 2-3, in which the IE SA also states that: 'while, subject to ongoing litigation in Norway, [Meta IE]'s Norwegian subsidiary is accruing liabilities on a daily basis by reference to the fine recently applied by NO SA, [Meta IE]'s processing operations as they relate to behavioural advertising remain unchanged at this point'.

⁵⁸ Letter of the IE SA to the NO SA of 13 October 2023, p. 3-6.

50. As mentioned above, on 26 September 2023, the NO SA used IMI to request the EDPB to adopt an urgent binding decision pursuant to Article 66(2) GDPR, with the effect of ordering the implementation of final measures (hereinafter, the '**NO SA Request to the EDPB**' or '**Request to the EDPB**').
51. Following the submission of the NO SA Request to the EDPB, the EDPB Secretariat assessed the completeness of the file on behalf of the Chair of the EDPB.
52. In the context of the assessment of the completeness of the file, the EDPB Secretariat contacted the NO SA on 4 October 2023 and 11 October 2023 requesting further documents and clarifications. In both cases, the NO SA responded on the same day by providing clarifications and uploading additional documents on IMI.
53. The EDPB Secretariat also contacted the IE SA on 5 October 2023, requesting additional documents and clarifications. Following a request sent by the IE SA to extend the deadline initially set on 6 October, the EDPB Secretariat extended the deadline to 9 October 2023. On 9 October, the IE SA replied by attaching some of the additional documents and providing some clarifications. On the basis of the reply, the EDPB Secretariat requested on the same day some further information and provided clarifications on the questions it had previously asked. On 10 October 2023, the IE SA responded to the EDPB Secretariat's email of 9 October 2023, highlighting the need for appropriate time to carry out verifications. On 11 October 2023, the EDPB Secretariat responded to the IE SA's email identifying certain items as matters of priority. On 12 October 2023, the IE SA responded to the EDPB Secretariat's request providing several documents and clarifications.
54. A matter of particular importance that was scrutinised by the EDPB Secretariat was the right to good administration, as required by Article 41 of the Charter of Fundamental Rights of the European Union (hereinafter, the '**Charter**'). Further details on this topic are provided in Section 3 of this urgent binding decision.
55. On 12 October 2023, the decision on the completeness of the file was then taken by the Chair of the EDPB and on 13 October 2023 by the NO SA in line with Article 13(2) of the EDPB RoP. The file was circulated by the EDPB Secretariat to all the members of the EDPB on 13 October 2023.
56. On 17 October 2023, following a request of the IE SA to include an additional letter sent by the IE SA to the NO SA on 13 October 2023, the EDPB decided to include it in the file, on the basis of Article 11(2) EDPB RoP.

2 COMPETENCE OF THE EDPB TO ADOPT AN URGENT BINDING DECISION UNDER ARTICLE 66(2) GDPR

57. The EDPB is competent to issue an urgent binding decision under Article 66(2) GDPR to the extent that the following conditions are met: an SA has taken provisional measures pursuant to Article 66(1) GDPR, and there is a request from this SA pursuant to Article 66(2) GDPR.⁵⁹
- 2.1 The SA has taken provisional measures under Article 66(1) GDPR**
58. On 14 July 2023, the NO SA adopted provisional measures pursuant to Article 66(1) GDPR, prohibiting Meta IE from processing the personal data of data subjects residing in Norway for targeting

⁵⁹ See Art. 66(2) GDPR and EDPB Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited (hereinafter '**EDPB Urgent Binding Decision 01/2021**'), adopted on 12 July 2021, section 2.

advertisements on the basis of observed behaviour for which Meta IE relies on Article 6(1)(b) GDPR or Article 6(1)(f) GDPR.

59. The EDPB therefore considers that this condition is satisfied.

2.2 Existence of a request pursuant to Article 66(2) GDPR coming from a SA in the EEA

60. On 26 September 2023, the NO SA requested the EDPB to adopt an urgent binding decision pursuant to Article 66(2) GDPR, by introducing a formal request in the IMI system (Article 17 of the EDPB RoP).

61. The EDPB therefore considers that this condition is satisfied.

2.3 Conclusion

62. The EDPB concludes it is competent to adopt an urgent binding decision under Article 66(2) GDPR.

3 THE RIGHT TO GOOD ADMINISTRATION

63. The EDPB is subject to Article 41 of the Charter (right to good administration). This is also reflected in Article 11(1) EDPB RoP.
64. Similarly to what is provided under Article 65(2) GDPR, an urgent binding decision of the EDPB is addressed to the lead supervisory authority and all the supervisory authorities concerned, and is binding on them⁶⁰. It is not aimed to address directly any third party.
65. Nevertheless, the EDPB assessed whether all the documents it received to be used in order to take its decision were known by Meta IE and Facebook Norway, and whether Meta IE and Facebook Norway were offered the opportunity to exercise their right to be heard on all the elements of fact and law to be used by the EDPB to take its decision.
66. In this respect, the NO SA informed the EDPB Secretariat that it made available all the documents it submitted to the EDPB to Meta IE and Facebook Norway. The other documents (submitted by the IE SA), if not already known to the companies, were made available to them by the EDPB Secretariat by way of letters of 13 October 2023⁶¹ and 18 October 2023⁶².
67. On 17 September 2023, the NO SA sent a letter to Meta IE and Facebook Norway asking for their submissions on its draft request for an Article 66(2) GDPR urgent binding decision from the EDPB. Following extensions of the deadline initially set, these submissions were provided on 26 September 2023 (hereinafter, '**Meta IE's Submissions of 26 September 2023**' and '**Facebook Norway's Submissions of 26 September 2023**'). These submissions also attached Meta IE's and Facebook Norway's previous submissions of 25 August 2023 concerning the intention of the NO SA to request an urgent binding decision of the EDPB ('**Meta IE's Submissions of 25 August 2023**' and '**Facebook Norway's Submissions of 25 August 2023**'). In addition to these submissions, the file submitted to the EDPB also included multiple documents produced by Meta IE and/or Facebook Norway in the context of the assessment of compliance with the IE SA Decisions and/or in the context of the legal proceedings

⁶⁰ Art. 65(2) GDPR. According to Art. 66(4) GDPR, this provision is derogated in respect of the deadline for adoption; therefore, the last sentence of Art. 65(2) GDPR fully applies.

⁶¹ Letter of the EDPB Chair to Meta IE and Facebook Norway of 13 October 2023.

⁶² Letter of the EDPB Chair to Meta IE and Facebook Norway of 18 October 2023.

concerning the NO SA Order⁶³, where Meta IE's and Facebook Norway's positions in respect of the elements being considered by the EDPB were clarified.

68. On the basis of the assessment performed by the EDPB Secretariat, Meta IE and Facebook Norway had not yet had an opportunity to make their views known on some elements of fact and law included in some documents of the file to be used by the EDPB to take its decision. The Chair of the EDPB invited by way of her letter of 13 October 2023⁶⁴ Meta IE and Facebook Norway to provide written submissions to the EDPB on these elements. These submissions, together with annexes, were provided by Meta IE and Facebook Norway on 16 October 2023 ('**Meta IE's Submissions of 16 October 2023**' and '**Facebook Norway's Submissions of 16 October 2023**')⁶⁵ and were subsequently added to the file.
69. On 18 October 2023, the Chair of the EDPB sent a new letter to Meta IE and Facebook Norway informing them of the document added to the file on 17 October 2023 and providing them with an opportunity to make written submissions on it. Meta IE and Facebook Norway made written submissions on 19 October 2023 ('**Meta IE and Facebook Norway's Submissions of 19 October 2023**'), which were added to the file.
70. The EDPB notes that Meta IE and Facebook Norway received the opportunity to make their views regarding all the legal and factual elements used by the EDPB to take this decision. Therefore, in case Meta IE and Facebook Norway would be found to be entitled to a right to be heard in this procedure, it would be in any case fully respected.

4 ON THE NEED TO REQUEST FINAL MEASURES

71. The EDPB considers that in order for an urgent binding decision adopted pursuant to Article 66(2) GDPR to order final measures two cumulative conditions need to be fulfilled: the existence of one (or several) infringement(s) and the existence of an urgency situation justifying a derogation from the regular cooperation procedure.
72. Consequently, the sections below assess first the existence of infringements (Section 4.1), then the existence of an urgency situation (Section 4.2).

4.1 On the existence of infringements

⁶³ By way of example, these documents included the Letter from Meta IE to the IE SA of 31 May 2023, the letter from Meta IE to the IE SA of 21 June 2023, the Letter from Meta IE to the IE SA of 30 June 2023, Meta IE's Response to the IE SA Provisional Position Paper of 4 August 2023, Letter from Meta IE to the IE SA of 27 July 2023, Letter from Meta IE to the NO SA of 27 July 2023.

⁶⁴ Letter of the Chair of the EDPB to Meta IE and Facebook Norway of 13 October 2023, replying to their letter of 28 September 2023 where they requested that Meta IE and Facebook Norway be granted access to any documents in the administrative file, and to be afforded an opportunity to make submissions after reviewing the file in advance of the EDPB reaching a final decision.

⁶⁵ On 18 October 2023, Meta IE and Facebook Norway provided new versions of two of their annexes. In these letters of 16 October 2023, Meta IE and Facebook Norway also informed the EDPB that they filed a complaint before the Oslo District Court challenging and seeking to invalidate the NO SA Order on the merits.

4.1.1 On the infringement of Article 6(1) GDPR

4.1.1.1 Summary of the overall position of the NO SA

73. The NO SA requested the EDPB to adopt an urgent binding decision ordering final measures to be taken across the EEA to ensure that '*personal data shall not be processed for behavioural advertising based on Article 6(1)(b) [GDPR] or Article 6(1)(f) GDPR in the context of the Services*'⁶⁶. In the NO SA Request to the EDPB, the NO SA defines '*behavioural advertising*' as '*targeting ads on the basis of observed behaviour*'⁶⁷. In the view of the NO SA, this includes '*targeting ads on the basis of inferences drawn from observed behaviour as well as on the basis of data subjects' movements, estimated location and how data subjects interact with ads and user-generated content*'⁶⁸. This definition is in line with their understanding of the scope of the IE SA Decisions⁶⁹.
74. In the NO SA Request to the EDPB, the NO SA states that '*[Meta IE] has failed to ensure compliance with (...) [the IE SA Decisions]*'⁷⁰. According to the NO SA, there is consensus among the CSAs that Meta IE's processing of personal data for behavioural advertising purposes is currently infringing the GDPR, and in particular Article 6(1)(b) GDPR, Article 6(1)(f) GDPR, and the duty to comply with the decisions of the SAs⁷¹.
75. The NO SA's analysis is based on the following elements:
- Despite the IE SA Decisions, Meta IE still relies on Article 6(1)(b) GDPR to process (1) location information, including GPS location, data subjects' activity on Meta products and the places data subjects like to go and the businesses and people data subjects are near; and (2) information about ads that Meta IE shows and how data subjects engage with those ads; for the purpose of behavioural advertising⁷².
 - Meta IE relies on Article 6(1)(f) GDPR to process some personal data for the purpose of behavioural advertising, while Article 6(1)(f) GDPR is not an appropriate legal basis for this processing⁷³.
 - The IE SA also considers that Meta IE failed to demonstrate that it has a lawful basis to process platform behavioural data for behavioural advertising⁷⁴, and did not provide any documentation confirming that it stopped processing personal data for the purpose of behavioural advertising on the basis of Article 6(1)(b) GDPR and Article 6(1)(f) GDPR⁷⁵.

⁶⁶ NO SA Request to the EDPB, p. 12.

⁶⁷ NO SA Request to the EDPB, p. 12.

⁶⁸ NO SA Request to the EDPB, p. 3-4, referring to the NO SA Order.

⁶⁹ NO SA Order, p. 3.

⁷⁰ NO SA Request to the EDPB, p. 6.

⁷¹ NO SA Request to the EDPB, p. 5-7.

⁷² NO SA Request to the EDPB, p. 4 which refers to the NO SA Order. See also NO SA Order, section 7.2.1.1.

⁷³ NO SA Request to the EDPB, p. 4. The NO SA Request to the EDPB only mentions that Meta IE changed its legal basis for '**some of its processing**' of personal data. Meta IE clarifies in its Letter to the IE SA of 30 June 2023 that these changes relate to the personal data collected on its products (paragraph 7c). A description of this data is provided in section 2.3 of the Meta IE Compliance Reports.

⁷⁴ NO SA Request to the EDPB, p. 5.

⁷⁵ NO SA's Decision to Impose a Coercive Fine on Meta IE and Facebook Norway of 7 August 2023, p. 4.

76. The NO SA states that Meta IE has already been given enough time to bring its processing into compliance with Article 6(1) GDPR, and takes the view that '*[Meta IE] is making use of dilatory strategies*'⁷⁶.
77. The NO SA considers that there is sufficient information to allow the EDPB to conclude that infringements are taking place⁷⁷.

4.1.1.2 Inappropriate reliance on Article 6(1)(b) GDPR

4.1.1.2.1 Summary of the position of the NO SA

78. The NO SA takes the view that Meta IE's infringement of Article 6(1)(b) GDPR in the context of its behavioural advertising processing activities was confirmed by the EDPB Binding Decisions and the IE SA Decisions which concluded, in line with the views expressed in previous EDPB guidelines, that Article 6(1)(b) GDPR is an unsuitable legal basis for behavioural advertising processing activities, both generally and in the case at issue⁷⁸.
79. The NO SA finds that Meta IE has incorrectly understood what constitutes '*processing of personal data for the purposes of behavioural advertising*' in the IE SA Decisions⁷⁹. It states that Meta IE's processing of data subjects' location data⁸⁰ and engagement with ads⁸¹ is part of Meta IE's processing of personal data for the purpose of behavioural advertising concerned by the IE SA Decisions⁸², and that, pursuant to those decisions, such processing which is based on Article 6(1)(b) GDPR, is unlawful⁸³.

4.1.1.2.2 Summary of the position of the controller

80. Meta IE states that, prior to the IE SA Decisions, it relied on Article 6(1)(b) GDPR in a good faith manner and its '*bona fide belief that it was lawful for it to do so*'⁸⁴, considering that different national courts found that Meta IE may validly rely on Article 6(1)(b) GDPR to process personal data for the purposes of behavioural advertising⁸⁵.

⁷⁶ NO SA Request to the EDPB, p. 6.

⁷⁷ NO SA Request to the EDPB, p. 7.

⁷⁸ NO SA Request to the EDPB, footnotes 4 and 10, referring to EDPB Guidelines 8/2020 on the targeting of social media users, paragraphs 49 and 71.

⁷⁹ NO SA Order, section 7.2.1.1, p. 14 (referring to the IE SA FB Decision paragraph 10.44(b) and the IE SA IG Decision paragraph 417(b), respectively).

⁸⁰ According to the NO SA, '*[Meta IE]'s use of location data to inform which ads are displayed to data subjects clearly constitutes Behavioural Advertising. It is unclear to us what this location is estimated on the basis of, if not the data subject's behaviour*'. NO SA Order, section. 7.2.1.1, p. 15.

⁸¹ According to the NO SA, '*For information about data subjects' engagement with ads, we understand that data subjects may click on "Hide Ad" and that one effect of this would be that the particular ad is not shown to that data subject again. We agree with [Meta IE]'s assertion set out in its letter of 30 June 2023 that this in itself does not constitute processing for Behavioural Advertising. However, to the extent that this or any other engagement with an ad is used to inform which other ads a data subject should see, we find that the processing of personal data does take place for Behavioural Advertising*', NO SA Order, section. 7.2.1.1, p. 15.

⁸² NO SA Order, section. 7.2.1.1, p. 15. The NO SA also states this in the NO SA Mutual Assistance Request, p. 5.

⁸³ NO SA Order, p. 15.

⁸⁴ Meta IE's Submissions of 25 August 2023, paragraph 65.

⁸⁵ Meta IE's Submissions of 25 August 2023, paragraph 65; Written Pleading of 18 August 2023 from Meta IE to Oslo District Court, p. 6.

81. Meta IE acknowledges that the IE SA Decisions concluded differently to these cases⁸⁶, and argues that it took since then substantial steps to bring its processing activities into ‘*what it believes was compliance with those decisions*’⁸⁷. Meta IE states that it changed its legal basis from Article 6(1)(b) GDPR to Article 6(1)(f) GDPR for the processing of personal data collected on Meta’s products for the purposes of behavioural advertising to comply with the IE SA Decisions⁸⁸. It states further that it relies on Article 6(1)(a) GDPR to process personal data obtained from third party advertising partners⁸⁹.
82. In relation to the definition of what behavioural advertising encompasses, Meta IE states that its processing of personal data for the purpose of behavioural advertising comprises the use of ‘*information collected on Meta’s products about a user’s behaviour over time in order to assess and understand users’ interests and preferences*’. According to Meta IE, this includes signals such as ‘*a user’s activity across Meta’s products, engagement with content such as other users’ posts or which pages they visit, the individuals and groups they communicate with, and/or what the user searches for*’⁹⁰. Meta IE states that it processes this personal data to assess and understand users’ interests and preferences, and to provide them with behavioural advertisements⁹¹.
83. However, Meta IE takes the view that its processing of a) demographic data (including location data), b) In-use app, browser and device data c) advertisement shown and d) advertisement interaction data⁹² does not constitute behavioural advertising, and therefore falls beyond the scope of the IE SA Decisions⁹³. In this respect, Meta IE argues that its processing of such data on the basis of Article 6(1)(b) GDPR is valid⁹⁴.

84.

⁹⁵.

4.1.1.2.3 Analysis of the EDPB

85. The EDPB Binding Decisions instructed, *inter alia*, the IE SA to find an infringement of Article 6(1) GDPR on the ground that Meta IE inappropriately relied upon Article 6(1)(b) GDPR to process personal data for the purposes of behavioural advertising, and therefore lacked a legal basis to process this data for this purpose⁹⁶. In relation to this, the EDPB also instructed the IE SA to include in each of its final

⁸⁶ Written Pleading of 18 August 2023 from Meta IE to Oslo District Court, p. 6.

⁸⁷ Meta IE’s Submissions of 25 August 2023, paragraph 65; Written Pleading of 18 August 2023 from Meta IE to Oslo District Court, p. 6.

⁸⁸ Meta IE Compliance Report on IE SA FB Decision, paragraphs 2.1 and 2.3 and Meta IE Compliance Report on IE SA IG Decision, paragraphs 2.1 and 2.3.

⁸⁹ Such data includes information from third party websites, apps and certain offline interactions (such as purchases). See Meta IE Letter to the IE SA of 30 June 2023, paragraph 7c and footnote 150 below.

⁹⁰ Meta IE Compliance Report on IE SA FB Decision, paragraph 2.2; Meta IE Compliance Report on IE SA IG Decision, paragraph 2.2

⁹¹ Meta IE Compliance Report on IE SA FB Decision, paragraph 2.2; Meta IE Compliance Report on IE SA IG Decision, paragraph 2.2.

⁹² As described in section 5.8.2 of the Meta IE Compliance Reports.

⁹³ Meta IE’s Request for preliminary injunction of 4 August 2023, p. 27.

⁹⁴ Meta IE’s Request for preliminary injunction of 4 August 2023, p. 27.

⁹⁵

⁹⁶ EDPB Binding Decision 3/2022, paragraphs 133 and 484; EDPB Binding Decision 4/2022, paragraphs 137 and 451.

- decisions an order for Meta IE to bring its processing of personal data for the purpose of behavioural advertising in the context of the Facebook and Instagram services into compliance with Article 6(1) GDPR within three months⁹⁷.
86. On the basis of the EDPB Binding Decisions, the IE SA Decisions ordered Meta IE to bring its processing into compliance with Article 6(1) GDPR⁹⁸, the IE SA ordered Meta IE to take the necessary actions to bring into compliance with Article 6(1) GDPR and to address the finding that Meta IE is not entitled to process personal data for the purpose of behavioural advertising on the basis of Article 6(1)(b) GDPR⁹⁹. The EDPB notes that the IE SA made clear that such action may include, but is not limited to, the identification of an appropriate alternative legal basis in Article 6(1) GDPR¹⁰⁰.
87. In the Compliance Reports, Meta IE indicated that it changed the legal basis it relies on for the processing of personal data collected on its products for behavioural advertising purposes from Article 6(1)(b) GDPR to Article 6(1)(f) GDPR as of 5 April 2023, which was the deadline for compliance with the IE SA Decisions¹⁰¹. Meta IE also states that it still relies on Article 6(1)(b) GDPR to process what it considers to be '*limited categories of non-behavioural information*' to show advertising on Facebook and Instagram¹⁰².
88. In the IE SA Final Position Paper assessing Meta IE's compliance with the IE SA Decisions and taking into consideration the comments received by the CSAs on such compliance, the IE SA addressed two key questions relevant for the purpose of this section of this urgent binding decision: the definition of behavioural advertising and whether the processing of Meta IE for advertising purposes relying upon Article 6(1)(b) GDPR falls within such definition¹⁰³.
89. As to the definition of behavioural advertising, the IE SA referred to the definition provided by the Article 29 Working Party in its Opinion 2/2010¹⁰⁴ being referred to by Meta IE in the Compliance Reports¹⁰⁵:
- 'Behavioural advertising is advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests'*¹⁰⁶.
-
- ⁹⁷ EDPB Binding Decision 3/2022, paragraphs 288 and 493; EDPB Binding Decision 4/2022, paragraphs 290 and 459.
- ⁹⁸ See IE SA FB Decision, paragraph 10.44b; IE SA IG Decision, paragraph 212. See also IE SA Final Position Paper, paragraph 2.1.
- ⁹⁹ IE SA FB Decision, paragraph 10.44b and IE SA IG Decision, paragraph 212.
- ¹⁰⁰ IE SA FB Decision, paragraph 10.44b and IE SA IG Decision, paragraph 212.
- ¹⁰¹ Meta IE Compliance Report on IE SA FB Decision, paragraph 2.1; Meta IE Compliance Report on IE SA IG Decision, paragraph 2.1.
- ¹⁰² Meta IE Compliance Report on IE SA FB Decision, paragraph 3.1.3; Meta IE Compliance Report on IE SA IG Decision, paragraph 3.1.3.
- ¹⁰³ IE SA Final Position Paper, paragraphs 7.3 - 7.22.
- ¹⁰⁴ IE SA Final Position Paper, paragraph 7.5, referring to Article 29 Working Party Opinion 2/2010 adopted on 22 June 2010, p. 5.
- ¹⁰⁵ Meta IE Compliance Report on IE SA FB Decision, p. 4; Meta IE Compliance Report on IE SA IG Decision, p.4.
- ¹⁰⁶ Article 29 Working Party Opinion 2/2010 adopted on 22 June 2010, p. 5.

90. To define whether the processing of Meta IE for advertising purposes relying upon Article 6(1)(b) GDPR falls within such definition, the IE SA also referred to the description of Meta IE's processing for behavioural advertising purposes provided by the EDPB in the EDPB Binding Decisions¹⁰⁷:

*'[Meta IE] collects data on its individual users and their activities on and off its Facebook social network service via numerous means such as the service itself, other services of the Meta group including Instagram, WhatsApp and Oculus, third party websites and apps via integrated programming interfaces such as Facebook Business Tools or via cookies, social plug-ins, pixels and comparable technologies placed on the internet user's computer or mobile device. According to the descriptions provided, [Meta IE] links these data with the user's Facebook account to enable advertisers to tailor their advertising to Facebook's individual users based on their consumer behaviour, interests, purchasing power and personal situation. This may also include the user's physical location to display content relevant to the user's location'*¹⁰⁸.

91. The IE SA noted that Meta IE relies on Article 6(1)(b) GDPR for a more limited set of personal data for advertising purposes in the Facebook and Instagram services¹⁰⁹. The EDPB notes that Meta IE argues that it is relying on Article 6(1)(b) GDPR for the processing of '*limited non-behavioural information*' to show advertisements, as described in its Compliance Reports¹¹⁰:

'a) Demographic data. This consists of age users provide, gender users provide, and estimated general location. The use of demographic data is required to ensure advertising is appropriate in accordance with the Terms of Use/Service. For example, (...) (c) relying on location is necessary to ensure advertisements that [Meta IE] show users are in an appropriate language and relate to an appropriately located company or service (e.g., [Meta IE] does not show users advertisements for products which are not available in their country);

'b) In-use app, browser and device data. (...) This includes the type of device being used, the language chosen on the device at that time and the version of the Facebook/Instagram app being used. These data points are necessary to deliver advertisements appropriately. For example, to properly format the advertisement to meet the viewing requirements of the device, to avoid users being shown advertisements for apps which are not supported by the operating system on their device, and ensure that the advertisement is in the chosen language of the user;

'c) Advertisements shown. This consists of information on whether the advertisement is rendered and delivered to a user. This information is a basic metric which [Meta IE] needs in order, for example, to ensure the number of advertisements that [Meta IE] shows to users is at an appropriate level and to ensure that the same advertisements are not being directed to the user repeatedly. The information does not indicate whether the user has actually noticed the advertisement;

'd) Advertisement interaction data. This consists of two forms of information provided by users if they choose to interact with advertisements: (a) to provide negative feedback on their advertising experience, for example by selecting to "hide" or report an advertisement; and (b)

¹⁰⁷ IE SA Final Position Paper, paragraph 7.4, referring to EDPB Binding Decision 3/2022, paragraphs 95-96 and EDPB Binding Decision 4/2022, paragraphs 98-99.

¹⁰⁸ EDPB Binding Decision 3/2022, paragraphs 95-96 and EDPB Binding Decision 4/2022, paragraphs 98-99.

¹⁰⁹ IE SA Final Position Paper, paragraphs 2.2, 4.5 and 7.6.

¹¹⁰ As referred to in the IE SA Final Position Paper, paragraph 7.6.

to provide positive feedback on their advertising experience, for example by clicking advertisements they find relevant'.¹¹¹

92. The EDPB notes the IE SA's following findings:

- In relation to location data, the IE SA took the view that Meta IE did not provide sufficient information to allow the IE SA to understand why location data would fall outside the definition of behavioural data¹¹². According to the IE SA, Meta IE did not explain whether it is processing the user's physical location or the location that they proactively provide to Meta IE to target ads to them.
- In relation to device data, the IE SA indicated that device information could also be used to identify different market segments, which in turn could be processed for behavioural advertising purposes¹¹³.
- In relation to advertisements shown, the IE SA indicated that more clarity from Meta IE would be required as to whether Meta IE only analyses records of ads shown (which, according to the IE SA, are not amounting to behavioural data) or also behavioural ads presented by other tools through a shared interface screen, which would also add to the behavioural processing by Meta IE¹¹⁴.
- In relation to advertisement interaction data, the IE SA underlined that 'interaction data' was listed in the definition of behavioural advertising in the Article 29 Working Party Opinion, which was incorporated by Meta IE into its Compliance Reports¹¹⁵. The IE SA therefore underlined the lack of clarity on how Meta IE would then distinguish 'advertisement interaction data', listed in point d) above from 'interaction data' included in the Article 29 Working Party Opinion 2/2010. The IE SA raised concerns as to the fact that Meta IE stated that it relies on Article 6(1)(b) GDPR in circumstances where the user provides positive advertising feedback¹¹⁶. According to the IE SA, this falls within the definition of behavioural

¹¹¹ Meta IE Compliance Report on IE SA FB Decision, paragraph 5.8.2; Meta IE Compliance Report on IE SA IG Decision, paragraph 5.8.2.

¹¹² In particular, the IE SA stated that '*[Meta IE] has explained the uses of this data, but not why these uses do not amount to behavioural processing. For example, it is unclear if location data is used by [Meta IE] to tailor ads to users on the basis of visits to certain types of shops, their travel to business hubs or holiday destinations, or the times of year at which they travel. If [Meta IE] use location data in these ways, then this would be processing personal data for the purposes of behavioural advertising, both by reference to the EDPB's description of such advertising, as set out at paragraph 7.4 above, and by reference to the Article 29 Working Party Opinion relied on by [Meta IE]', IE SA Final Position Paper, paragraph 7.11.*

¹¹³ The IE SA stated that '*it is unclear whether [Meta IE] identifies device information as a different market segment. While the processing of device information to serve ads may not amount to behavioural advertising, it is possible that [Meta IE] identifies certain devices as a different market segment. The type of device could indicate spending power or history, which could be processed for behavioural purposes', IE SA Final Position Paper, paragraph 7.12.*

¹¹⁴ IE SA Final Position Paper, paragraph 7.13.

¹¹⁵ Article 29 Working Party Opinion 2/2010 adopted on 22 June 2010, p. 5 referred to in Meta IE Compliance Report on IE SA FB Decision, p. 4 and Meta IE Compliance Report on IE SA IG Decision, p. 4.

¹¹⁶ The IE SA's concerns relate in particular to Meta IE's statement that when '*the user provides positive advertising feedback (e.g., actively choosing to click on a specific ad they find relevant and want to see), [Meta IE] similarly needs to use that information to ensure it is providing the user with an appropriate and relevant personalised advertising experience pursuant to the Terms of Service', see IE SA Final Position Paper, paragraph 7.14, referring to Meta IE Compliance Report on IE SA FB Decision, paragraph 5.8.2 and Meta IE Compliance Report on IE SA IG Decision, paragraph 5.8.2.*

advertising provided by the Article 29 Working Party Opinion 2/2010 as it involves Meta IE '*inferring conclusions about user preferences from users' interaction with an advertisement*'¹¹⁷. Following further information provided by Meta IE on 30 June 2023 to the IE SA on negative advertising feedback¹¹⁸, the IE SA indicated that, to the extent that Meta IE '*processes personal data solely to prevent a specific hidden ad being shown to a user, then the [IE SA] agrees that this does not amount to behavioural advertising. However, to the extent that [Meta IE] infers a user's advertising preferences from the fact that they have hidden an ad, then this does fall within the definition of behavioural advertising*'¹¹⁹. The IE SA added that '*[Meta IE] submissions are too vague to determine whether it processes personal data just to hide the specific ad, or whether it draws inferences from the choice to hide an ad. The reference in the justification of this processing to a user's "personal advertising experience" indicates that the decision to hide one ad could be used to infer preferences about the ads that a user receives more generally*'¹²⁰. The EDPB notes that this appreciation is in line with the observations made by the DE Hamburg SA¹²¹. The IE SA therefore provided that '*it appears from the information provided by [Meta IE] that it uses data about hidden ads to engage in behavioural advertising*'. The IE SA also provided similar conclusions for the positive feedback, raising that '*Using information about click-throughs to determine what types of ads a user wants to see in the future falls plainly within the definition of behavioural advertising provided by [Meta IE] to the [IE SA]*'¹²².

93. In light of the above, the EDPB notes that the IE SA found that Meta IE still conducts some processing for the purposes of behavioural advertising in reliance on Article 6(1)(b) GDPR¹²³.
94. In addition, the IE SA also indicated the lack of sufficient information to explain why categories (a) to (d) were not behavioural data¹²⁴. The EDPB also notes that on this basis, the IE SA found that Meta IE had not demonstrated compliance with the IE SA Decisions as regards reliance on Article 6(1)(b) GDPR for behavioural advertising¹²⁵.
95. The EDPB notes that this view was also expressed by certain CSAs replying to the IE SA IMI Informal Consultations. More specifically, the FI SA stated that '*the following personal data seems to be still unlawfully collected for behavioural advertising purposes under Article 6(1)(b) [GDPR]: "Information*

¹¹⁷ IE SA Final Position Paper, paragraph 7.15.

¹¹⁸ Meta IE said that '*with respect to negative advertising feedback, if a user selects the option that is available to "Hide Ad – never see this ad again," then [Meta IE] needs to use that information to ensure that choice regarding the user's personal advertising experience (i.e., what advertisements they do not want to see) is respected*', IE SA Final Position Paper, paragraph 7.16.

¹¹⁹ IE SA Final Position Paper, paragraph 7.16, referring to the comments of the DE Hamburg SA on the IE SA Provisional Position Paper.

¹²⁰ IE SA Final Position Paper, paragraph 7.16.

¹²¹ '*Allowing [Meta IE] to further justify whether it processes personal data only to hide a particular ad, or whether it draws inferences from the decision to hide an ad, is nothing more than leaving a choice not to describe the actual purpose of the processing, to formally fall short of the definition of behavioural advertising. In doing so, hiding certain ads without anything deriving from that decision would contradict [Meta IE]'s business model. To the extent that this or other engagement with an ad is used to learn what other ads a data subject should see, Hamburg SA notes that the processing of personal data serves purposes of behavioural advertising*', Views of DE Hamburg SA of 4 May 2023; as referred to in the IE SA Final Position Paper, paragraph 7.17.

¹²² IE SA Final Position Paper, paragraph 7.19.

¹²³ IE SA Final Position Paper, paragraph 6.2 and paragraph 8.1.

¹²⁴ IE SA Final Position Paper, paragraph 7.22.

¹²⁵ IE SA Final Position Paper, paragraphs 7.1, 7.22 and 8.1.

*about ads we show you and how you engage with those ads” and “Location information”*¹²⁶. The IT SA also stated that ‘[Meta IE]’s proposal is not such as to adequately implement the order to bring the processing into compliance insofar as it misclassifies part of the user-related information and thereby applies the legal basis of contractual performance under Article 6(1)(b) GDPR to the serving of ads which, actually, are behavioural in nature’¹²⁷.

96. The EDPB observes that if any of the data listed in paragraph 91 of this urgent binding decision may be considered as falling within the scope of the definition of behavioural advertising, there are grounds for finding that Meta IE is infringing Article 6(1) GDPR. This is because Meta IE would still be processing personal data for the purpose of behavioural advertising on the basis of Article 6(1)(b) GDPR, although it was considered unlawful by the IE SA Decisions¹²⁸.
97. In this respect, the EDPB shares the IE SA’s view that Meta IE still conducts some processing of personal data for the purposes of behavioural advertising in reliance on Article 6(1)(b) GDPR¹²⁹, at least for the following categories of data:
 - **Location data** - the EDPB finds, in line with the view of the IE SA, that Meta IE failed to demonstrate that its processing of location data does not constitute processing for the purpose of behavioural advertising¹³⁰. It is unclear to the EDPB, as it is to the NO SA and the IE SA, on which basis the location is estimated, if not the data subject’s behaviour. The EDPB consequently finds, in line with the view of the NO SA, that Meta IE’s processing of location data to inform which ads are displayed to data subjects constitutes behavioural advertising¹³¹.
 - **Advertisement interaction data** - the EDPB finds, in line with the view of the IE SA, that Meta IE failed to demonstrate that its processing of advertisement interaction data does not constitute processing for the purpose of behavioural advertising. The EDPB shares the view of the IE SA that ‘[Meta IE] is recording the behaviour of the users when they are presented with ads and use that to tailor future presentation of ads’¹³². The EDPB consequently finds that Meta IE’s processing of advertisement interaction data constitutes behavioural advertising for the following reasons:
 - As rightly pointed out by the IE SA, the EDPB recalls that interaction is listed among the data types in the definition of behavioural advertising in the Article 29 Working Party Opinion 2/2010¹³³.
 - The EDPB observes that irrespective of whether the data subject provides negative or positive feedback on the ads they see, Meta IE states that the interactions will be used to provide an ‘appropriate and relevant advertising experience’¹³⁴ which indicates that Meta IE is inferring conclusions about user preferences from such interaction.

¹²⁶ Views of the FI SA of 15 May 2023, p. 2.

¹²⁷ Views of IT SA on IE SA FB Decision of 23 May 2023, p. 2, and views of IT SA in IE SA IG Decision of 23 May 2023, p. 2.

¹²⁸ In this respect, the IE SA Decisions implemented the findings described in the EDPB Binding Decision 3/2022, paragraphs 94-133 and the EDPB Binding Decision 4/2022, paragraphs 97-137.

¹²⁹ See paragraphs 92-93 above.

¹³⁰ IE SA Final Position Paper, paragraph 7.11.

¹³¹ IE SA Final Position Paper, paragraph 7.11.

¹³² IE SA Final Position Paper, paragraph 7.14.

¹³³ IE SA Final Position Paper, paragraph 7.14.

¹³⁴ Meta IE Compliance Report on IE SA FB Decision, p. 16.

- With respect to negative feedback (i.e., where the data subject clicks to hide/report an ad), the EDPB observes that Meta IE states that it needs to use this information ‘*to ensure that choice regarding the user’s personal advertising experience (i.e., what advertisements they do not want to see) is respected*’¹³⁵. The EDPB also observes that Meta IE states that the options ‘*Hide Ad*’ and ‘*Report Ad*’ are used to ‘*directly influence the ads [users] see*’¹³⁶. The EDPB shares the view of the IE SA that ‘*the reference in the justification of this processing to a user’s “personal advertising experience” indicates that the decision to hide one ad could be used to infer preferences about the ads that a user receives more generally*’¹³⁷ and therefore that ‘*it appears from the information provided by [Meta IE] that it uses data about hidden ads to engage in behavioural advertising*’¹³⁸.
 - With respect to positive feedback, the EDPB observes that Meta IE states that when ‘*the user provides positive advertising feedback (e.g., actively choosing to click on a specific ad they find relevant and want to see), [Meta IE] similarly needs to use that information to ensure it is providing the user with an appropriate and relevant personalised advertising experience pursuant to the Terms of Service*’¹³⁹. Consequently, the EDPB also shares the view of the IE SA that this practice falls within the definition of behavioural advertising provided by the WP29 Opinion as it involves Meta IE ‘*inferring conclusions about user preferences from users’ interaction with an advertisement*’¹⁴⁰.
98. In conclusion, the EDPB finds that Meta IE is inappropriately relying on Article 6(1)(b) GDPR to process location data and advertisement interaction data collected on its products for the purpose of behavioural advertising.
99. In addition, the EDPB shares the view of the IE SA that Meta IE did not provide sufficient information to explain why other categories of data processed by Meta IE do not amount to behavioural data, such as device data and advertisements shown¹⁴¹. In this respect, the EDPB finds, in line with the view of the IE SA, that in relation to device data, if Meta IE would use device data to identify different market segments, this would constitute a processing for behavioural advertising for which it would rely inappropriately on Article 6(1)(b), infringing Article 6(1) GDPR¹⁴².

¹³⁵ Letter from Meta IE to the IE SA of 30 June 2023, p. 5.

¹³⁶ Meta IE’s submissions of 16 October 2023 to the Oslo District Court. For Instagram specifically, also see the screenshots included in p. 35 of the Annex 3 to the Compliance Report on IE SA IG Decision.

¹³⁷ IE SA Final Position Paper, paragraph 7.16.

¹³⁸ IE SA Final Position Paper, paragraph 7.18.

¹³⁹ Meta IE Compliance Report on IE SA FB Decision, paragraph 5.8.2 and Meta IE Compliance Report on IE SA IG Decision, paragraph 5.8.2.

¹⁴⁰ IE SA Final Position Paper, paragraph 7.15.

¹⁴¹ See paragraph 89 above.

¹⁴² The IE SA stated that ‘*it is unclear whether [Meta IE] identifies device information as a different market segment. While the processing of device information to serve ads may not amount to behavioural advertising, it is possible that [Meta IE] identifies certain devices as a different market segment. The type of device could indicate spending power or history, which could be processed for behavioural purposes*’, IE SA Final Position Paper, paragraph 7.12.

4.1.1.3 Inappropriate reliance on Article 6(1)(f) GDPR

4.1.1.3.1 Summary of the position of the NO SA

100. The NO SA considers that Article 6(1)(f) GDPR does not constitute an appropriate legal basis under Article 6(1) GDPR for Meta IE's behavioural advertising processing¹⁴³.
101. The NO SA refers to the IE SA Final Position Paper, in which the IE SA concluded that Meta IE continues to fail to rely on a valid legal basis to process personal data for behavioural advertising purposes under Article 6(1) GDPR, despite Meta IE's switch to Article 6(1)(f) GDPR as a legal basis for its behavioural advertising processing on 5 April 2023¹⁴⁴. The NO SA outlines that this conclusion was supported by several CSAs explicitly, without any objection being raised by the other CSAs¹⁴⁵.
102. Further, the NO SA states that paragraph 117 of the CJEU Bundeskartellamt Judgment validates the conclusion that Article 6(1)(f) GDPR does not constitute an appropriate legal basis for Meta IE's behavioural advertising processing¹⁴⁶. In this respect, the NO SA acknowledges Meta IE's view that the judgment is irrelevant and relates to a different aspect of Meta IE's processing for behavioural advertising¹⁴⁷. However, the NO SA argues that the ruling does apply to Meta IE's behavioural advertising practices in general and, therefore, that it cannot be disregarded¹⁴⁸.

4.1.1.3.2 Summary of the position of the controller

103. In its Compliance Reports, Meta IE states that it has changed its legal basis from Article 6(1)(b) GDPR to Article 6(1)(f) GDPR for 'Behavioural Advertising Processing' - solely for personal data collected on Meta's products¹⁴⁹ - to comply with the IE SA Decisions¹⁵⁰.
104. As mentioned in paragraph 81 above, Meta IE defines the scope of this processing operation processed on the basis of Article 6(1)(f) GDPR as follows:

'Behavioural Advertising Processing comprises the use by [Meta IE] of information collected on [Meta's] products about a user's behaviour over time in order to assess and understand users'

¹⁴³ NO SA Request to the EDPB, p. 4.

¹⁴⁴ NO SA Request to the EDPB, p. 5. As specified in paragraph 104 below, Meta IE defines the scope of this processing operation processed on the basis of Art. 6(1)(f) GDPR as relating to personal data collected on Meta's products.

¹⁴⁵ NO SA Request to the EDPB, p. 5.

¹⁴⁶ NO SA Request to the EDPB, p. 5.

¹⁴⁷ NO SA Request to the EDPB, p. 6. As specified in paragraphs 109 and 142 below, in paragraph 1.5 (A) of Meta IE's Response to the IE SA's Provisional Position Paper of 4 August 2023, Meta IE considers that the Bundeskartellamt Judgment 'does not rule out Article 6(1)(f) [GDPR] "as a matter of principle" as a valid legal basis for [Meta IE]'s Behavioral Advertising Processing. The judgment assessed Article 6(1)(f) [GDPR] (and the element of "necessity") in the context of different processing than is at-issue here (i.e., data collected off-[Meta], and to a limited extent cross-product data processing, as opposed to data collected on-[Meta] products). (...) Further, the CJEU did not (and could not as a matter of law) issue a blanket finding that users' interests will always outweigh [Meta IE]'s and third parties' legitimate interests in the context of personalised advertising (...).'

¹⁴⁸ NO SA Request to the EDPB, p. 6.

¹⁴⁹ Meta IE indicates to rely on Art. 6(1)(a) GDPR to process personal data about users' activity off-Meta's products (such as on third-party websites, apps and certain offline interactions (e.g., purchases)), obtained by Meta IE from third party advertising partners for the purposes of showing personalised advertising to these users on Facebook or Instagram (see Meta IE Compliance Report on IE SA FB Decision, p. 12, paragraph 3.1.2, and Meta IE Compliance Report on IE SA IG Decision, p. 13, paragraph 3.1.2).

¹⁵⁰ Meta IE Compliance Report on IE SA FB Decision, p. 4, and Meta IE Compliance Report on IE SA IG Decision, p. 4.

*interests and preferences. This includes signals such as a user's activity **across [Meta's] products**, engagement with content such as other users' posts or which pages they visit, the individuals and groups they communicate with, and/or what the user searches for. [Meta IE] uses all of these signals to assess and understand users' interests and preferences and to provide them with behavioural advertisements.'* (emphasis added in bold)¹⁵¹

105. With respect to the above, the EDPB notes that the personal data processed for behavioural advertising purposes on the basis of Article 6(1)(f) GDPR is collected 'on' and 'across' Meta's products and that these terms are used interchangeably by Meta IE.
106. Meta IE also refers to its updated privacy policies for Facebook and Instagram, which provide the list of categories of personal data processed for this purpose¹⁵².
107. In Meta IE's view, it was entitled to consider that it could switch to Article 6(1)(f) GDPR for its behavioural advertising processing to comply with the IE SA Decisions¹⁵³. According to Meta IE, neither the EDPB Binding Decisions nor the IE SA Decisions ordered Meta IE to rely on a specific legal basis under Article 6(1) GDPR, such as Article 6(1)(a) GDPR¹⁵⁴. Meta IE argues that it is only once the IE SA adopted the IE SA Final Position Paper on 18 August 2023 that an authority concluded that Meta IE's reliance on Article 6(1)(f) GDPR was insufficient to comply with the IE SA Decisions¹⁵⁵. Meta IE argues that prior to this date '*[s]ome SA submissions are inconsistent with one another and cannot be reconciled (for example (...) certain SAs appear to consider that consent is the only viable basis possible whereas others accept Article 6(1)(f) GDPR is viable*'¹⁵⁶.
108. Meta IE carried out Legitimate Interests Assessments annexed to its Compliance Reports¹⁵⁷, in which it concludes that Article 6(1)(f) GDPR constitutes an appropriate legal basis for behavioural advertising¹⁵⁸. Meta IE reiterates this conclusion on 4 August 2023, after having made a commitment to switch to Article 6(1)(a) GDPR through the Meta IE's Consent Proposal¹⁵⁹. In addition, Meta IE highlighted that it '*expended significant resources*' and implemented '*very substantial steps*' to switch from Article 6(1)(b) GDPR to Article 6(1)(f) GDPR to comply with the deadline of 5 April 2023¹⁶⁰.
109. With respect to the CJEU Bundeskartellamt Judgment, Meta IE takes the view that this case '*does not rule out Article 6(1)(f) [GDPR] as a matter of principle as a valid legal basis*' for Meta IE's behavioural

¹⁵¹ Meta IE Compliance Report on IE SA FB Decision, p. 4, and Meta IE Compliance Report on IE SA IG Decision, p. 4.

¹⁵² Meta IE Compliance Report on IE SA FB Decision, p. 4-5, and Meta IE Compliance Report on IE SA IG Decision, p. 4-5.

¹⁵³ Meta IE's Submissions of 26 September 2023, p. 10, and Meta IE's Submissions of 25 August 2023, p. 22. See also Meta IE's letter to the IE SA of 27 July 2023, p. 1-2.

¹⁵⁴ Meta IE's Submissions of 26 September 2023, p. 10, and Meta IE's Submissions of 25 August 2023, p. 4 and 16.

¹⁵⁵ Meta IE's Submissions of 26 September 2023, p. 11 and Meta IE's Submissions of 16 October 2023, p.5.

¹⁵⁶ Letter from Meta IE to the IE SA regarding process and urgency of 31 May 2023, p. 3.

¹⁵⁷ Meta IE's Legitimate Interests Assessments Behavioural Advertising Processing of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision.

¹⁵⁸ Annex 4 to the Meta IE Compliance Report on IE SA FB Decision and to Meta IE Compliance Report on IE SA IG Decision, p. 4, and Meta IE Compliance Report on IE SA FB Decision, p. 11, Meta IE Compliance Report on IE SA IG Decision, p. 12.

¹⁵⁹ Meta IE's Request for preliminary injunction, 4 August 2023, p. 27.

¹⁶⁰ Meta IE's Submissions of 26 September 2023, p. 10 and Meta IE's Submissions of 16 October 2023, p.5. See also Meta IE's Submissions of 25 August 2023, p. 33.

advertising processing activities, given that the CJEU ‘*did not (and could not as a matter of law) issue a blanket finding that users’ interests will always outweigh [Meta IE]’s and third parties’ legitimate interests in the context of personalised advertising*’¹⁶¹. It argues that the CJEU Bundeskartellamt Judgment relates to a different processing than the processing covered by the EDPB Binding Decisions and the IE SA Decisions. More specifically, Meta IE points out that this judgment relates to personal data collected off-Meta, as opposed to data collected on-Meta products. Notably, Meta IE states that the scope of the case, ‘*excludes processing for behavioural advertising purposes when using personal data collected across different [Meta IE]’s products*’, while acknowledging that the case focuses ‘*to a lesser extent*’ on ‘*the processing of personal data collected across various [Meta IE]’s products*’¹⁶².

110. Lastly, despite considering that it can lawfully rely on Article 6(1)(f) GDPR, Meta IE announced that, taking into account the ‘*different views*’ of the IE SA both in the IE SA Provisional Position Paper and regarding the interpretation of the CJEU Bundeskartellamt Judgment, it was willing to switch to consent for the processing at stake¹⁶³.

[REDACTED]
164.

[REDACTED]
165.

[REDACTED]
166.

[REDACTED]
167.

4.1.1.3.3 Analysis of the EDPB

111. In the IE SA Decisions, Meta IE was directed to take the necessary action to address the finding that Meta IE is not entitled to carry out the processing operations at stake on the basis of Article 6(1)(b) GDPR, was ordered to bring its processing of personal data for the purposes of behavioural advertising into compliance with Article 6(1) GDPR and it was specified that such action is ‘*not limited to the*

¹⁶¹ Meta IE’s Response to IE SA’s Provisional Position Paper, 4 August 2023, section 1.5 (A) and also section 2 for a more detailed analysis.

¹⁶² Meta IE’s Request for preliminary injunction, 4 August 2023, p. 27.

¹⁶³ Meta IE’s letter to the IE SA of 27 July 2023, p. 1-2.

[REDACTED]
¹⁶⁴ Meta IE’s letter to the IE SA of 27 July 2023, p. 2.

¹⁶⁵ Meta IE’s letter to the IE SA of 27 July 2023, p. 2.

¹⁶⁶ IE SA’s letter to Meta IE of 11 August 2023, p. 2.

¹⁶⁷ IE SA’s letter to Meta IE of 11 August 2023, p. 2.

identification of an appropriate alternative legal basis', but may include the implementation of '*any necessary measures required to satisfy the conditionality associated with that/those alternative legal basis/bases*'¹⁶⁸.

112. The EDPB notes that, according to Meta IE Compliance Reports and the IE SA Final Position Paper, Meta IE relies on Article 6(1)(f) GDPR to process personal data collected on Meta's products¹⁶⁹ for the purposes of behavioural advertising since 5 April 2023¹⁷⁰.
113. Pursuant to Article 6(1)(f) GDPR, Recital 47 GDPR and the CJEU's settled case-law¹⁷¹, **three cumulative conditions** must be met to be able to rely on Article 6(1)(f) GDPR, '*namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, [according to a balancing test] that the interests or fundamental freedoms and rights of the person concerned by the data protection do not take precedence over the legitimate interest of the controller or of a third party*'¹⁷².
114. More specifically, **the first condition relates to the existence of legitimate interests pursued by the controller or a third party**.
115. Meta IE has identified different interests that it considers legitimate and on which it relies for the processing at stake. These interests are pursued either by Meta IE or third parties, namely businesses that use Facebook/Instagram and other users of Meta's products¹⁷³. More specifically, Meta IE identified the four following legitimate interests:
 - (1) Meta IE's '*interest and the interests of other users to provide a positive user experience that users will want to engage with, and which is tailored to users - providing quality targeted and personalised ads is a core element of the wider user experience across Meta Products*',
 - (2) Meta IE's '*interest and the interests of other users to enable [Meta IE] to generate revenue and continue to innovate, improve and develop the Meta Products and new technologies*',
 - (3) Meta IE's and third parties' (e.g. advertisers) interests '*to provide businesses, both big and small, the opportunity to connect with the users who are most likely to be interested in their products and services*', and
 - (4) Meta IE's '*interests and the interests of third parties (e.g. advertisers) and other users, for businesses, both big and small, to be able to promote their products and services to users*'¹⁷⁴.

¹⁶⁸ IE SA FB Decision, paragraph 8; and IE SA IG Decision, paragraph 212.

¹⁶⁹ IE SA Final Position Paper, paragraph 7.23, p. 11-12, referring to Meta IE's Letter to the IE SA of 30 June 2023, and Meta IE Compliance Report on IE SA FB Decision, p. 4, and Meta IE Compliance Report on IE SA IG Decision, p. 4.

¹⁷⁰ IE SA Final Position Paper, paragraph 7.25, p. 12, and Meta IE Compliance Report on IE SA FB Decision, p. 4, and Meta IE Compliance Report on IE SA IG Decision, p. 4.

¹⁷¹ As recently recalled in the CJEU Bundeskartellamt Judgment, paragraph 106, which refers to previous case-law. The IE SA Final Position Paper also recalls and applies this test in paragraphs 7.27 and seq., p. 12-21.

¹⁷² See paragraph 106 of the CJEU Bundeskartellamt Judgment.

¹⁷³ Meta IE Compliance Report on IE SA FB Decision, p. 6, and Meta IE Compliance Report on IE SA IG Decision, p. 6.

¹⁷⁴ Meta IE Compliance Report on IE SA FB Decision, p. 6, and Meta IE Compliance Report on IE SA IG Decision, p. 6.

116. These four categories of interests are further broken down in several sub-interests in Meta IE Legitimate Interests Assessments¹⁷⁵. For example, the first and the second legitimate interests also include the following sub-interest: '[For other Facebook and Instagram users:] *The enjoyment of Facebook and Instagram services free of charge*'.¹⁷⁶
117. As recalled by the IE SA, the given legitimate interests must be '*sufficiently clearly articulated and [be] real and present, corresponding to current activities or to benefits that are expected in the near future*'¹⁷⁷.
118. The EDPB notes that the IE SA concluded that the interests listed by Meta IE in its Compliance Reports can meet these criteria¹⁷⁸.
119. **The second condition relates to the necessity of the processing for the pursuit of those interests (or ‘necessity test’).**
120. In its Compliance Reports, Meta IE considers that: (1) the processing at stake is necessary to pursue and achieve the legitimate interests identified by Meta IE¹⁷⁹, (2) this processing is reasonable and proportionate to achieve the legitimate interests pursued¹⁸⁰ and (3) no viable alternatives exist that would allow the legitimate interests to be achieved¹⁸¹.
121. In that regard, the IE SA considers that Meta IE failed to demonstrate in its Compliance Reports that its behavioural advertising processing was necessary to the different legitimate interests it identified¹⁸². More specifically, the IE SA points out that Meta IE's explanations regarding the impact of the processing at stake are '*too vague*' and therefore they do not allow the IE SA to determine that there is a less intrusive alternative that Meta IE could pursue¹⁸³. In addition, the IE SA considers that Meta IE Legitimate Interests Assessments do not apply the necessity test for each of the legitimate interest on which it relies¹⁸⁴.
122. More specifically, regarding the first interest set out by Meta IE, the IE SA refers to the EDPB Binding Decision 3/2022 and concludes that behavioural advertising is not in the interest of *all* Meta IE's users, but only of *some* users¹⁸⁵. Therefore, according to the IE SA, Meta IE has not explained the need to

¹⁷⁵ Meta IE Legitimate Interests Assessments Behavioural Advertising Processing of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision, p. 9-13.

¹⁷⁶ Meta IE Legitimate Interests Assessments Behavioural Advertising Processing of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision, p. 9. This sub-interest is further detailed on p. 12 of Meta's Legitimate Interests Assessments.

¹⁷⁷ IE SA Final Position Paper, paragraph 7.33, referring to the EDPB Binding Decision 02/2022, paragraph 110.

¹⁷⁸ IE SA Final Position Paper, paragraph 7.33, p. 13-14.

¹⁷⁹ Meta IE Compliance Report on IE SA FB Decision, p. 6 and Meta IE Compliance Report on IE SA IG Decision, p.6, both referring to sections 2.b, 2.c., and 3.a of Meta IE Legitimate Interests Assessments.

¹⁸⁰ Meta IE Compliance Report on IE SA FB Decision, p. 6 and Meta IE Compliance Report on IE SA IG Decision, p. 7, both referring to section 3.b of Meta IE Legitimate Interests Assessments.

¹⁸¹ Meta IE Compliance Report on IE SA FB Decision, p. 6 and Meta IE Compliance Report on IE SA IG Decision, p. 7, both referring to sections 3.c, 3.d, and 3.e of Meta IE Legitimate Interests Assessments.

¹⁸² IE SA Final Position Paper, paragraph 7.50, p. 18.

¹⁸³ IE SA Final Position Paper, paragraph 6.3, p. 5.

¹⁸⁴ IE SA Final Position Paper, paragraph 7.41, referring to Meta IE Legitimate Interests Assessments Behavioural Advertising Processing of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision.

¹⁸⁵ IE SA Final Position Paper, paragraphs 7.43-7.44, p. 16.

process the personal data of all of its users '*for the purposes of realising the interests of those users who want to receive behavioural advertising*'¹⁸⁶.

123. Further, regarding the second, third and fourth interests put forward by Meta IE in its Compliance Reports¹⁸⁷, the IE SA concludes that Meta IE's arguments are not sufficiently substantiated because of the vagueness and the lack of specificity of the analysis¹⁸⁸. In particular, Meta IE has not explained which specific categories of personal data Meta IE needs to process or which processing operations need to take place to achieve the above interests¹⁸⁹.
124. When conducting the 'necessity test' in the Meta IE Legitimate Interests Assessments, Meta IE claims that '*Without the Processing, which as explained above is essential in order to monetise Facebook and Instagram, [Meta IE] would not be able to provide the services to users free of charge in the same manner as it does currently. This in turn would jeopardise the attainment of the legitimate interests identified above*'¹⁹⁰. According to Meta IE, if it did not carry out the processing of personal data collected on its products for the purpose of behavioural advertising and if it only carried out the 'limited' processing it engages in when data subjects object, it '*would significantly impact the user experience on Facebook and Instagram (in part, due to less innovation happening on the platforms due to reduced revenue) and it would also impact [Meta IE]'s ability to provide Facebook and Instagram free of charge (regardless of the financial means of the user) to users as this is largely due to the revenues that [Meta IE] makes from enabling advertisers to effectively advertise to Instagram and Facebook users*'¹⁹¹.
125. However, the IE SA points out that Meta IE's privacy policy states that Meta IE is pursuing a legitimate interest '*to generate revenue*', which is different than providing services for free¹⁹². According to the IE SA, given that other types of advertising may also generate revenue, it cannot be concluded that behavioural advertising is necessary to generate '*any revenue at all*'¹⁹³.
126. The IE SA also highlights that '*there is no explanation as to why it is necessary to process all the data categories that [Meta IE] uses for behavioural advertising in order to provide the services for free*'¹⁹⁴. Against this background, the IE SA concludes that Meta IE's claim that it is necessary to carry out behavioural advertising to provide Meta IE's services is not sufficiently granular¹⁹⁵. In particular, it is unclear whether, through this argument, Meta IE is saying that (1) Meta IE is unable to provide Facebook and Instagram for free unless it processes the personal data of *all* of its users for the purpose

¹⁸⁶ IE SA Final Position Paper, paragraph 7.44, p. 16.

¹⁸⁷ Meta IE Compliance Report on IE SA FB Decision, p. 6, and Meta IE Compliance Report on IE SA IG Decision, p. 6.

¹⁸⁸ IE SA Final Position Paper, paragraphs 7.45 and 7.50, p. 16 and 18.

¹⁸⁹ IE SA Final Position Paper, paragraph 7.45, p. 16.

¹⁹⁰ Meta IE Legitimate Interests Assessments Behavioural Advertising Processing of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision, p. 21, section 3a.

¹⁹¹ Meta IE Legitimate Interests Assessments Behavioural Advertising Processing of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision, p. 24, section 3d.

¹⁹² IE SA Final Position Paper, paragraph 7.46, p. 17.

¹⁹³ IE SA Final Position Paper, paragraph 7.46, p. 17.

¹⁹⁴ IE SA Final Position Paper, paragraph 7.47, p. 17.

¹⁹⁵ IE SA Final Position Paper, paragraph 7.47, p. 17.

of behavioural advertising, or (2) Meta IE is still able to provide Facebook and Instagram for free by processing the personal data of *some* of its users who do not object to behavioural advertising¹⁹⁶.

127. The IE SA's conclusion for the second condition was shared by a number of CSAs in their comments and reactions on the Compliance Reports:

- On 4 May 2023, the NL SA outlined that '*[t]he massive processing of users' (special) personal data for the purpose of behavioural advertising is not 'necessary' for the purposes of the declared interests*'¹⁹⁷.
- On 23 May 2023, the IT SA notes in relation to Meta IE Legitimate Interests Assessments that '*it is as if the controller were shifting the burden of proof regarding legitimate interest as the legal basis of processing on the data subjects – who conversely should be called into play as key actors in the two subsequent steps of the legitimate interest test, i.e. when assessing the necessity of the processing and performing the required balancing exercise*'¹⁹⁸.
- In the NO SA Order, the NO SA argues that Meta IE fails to show that it fulfils the 'necessity test' based on (1) the absence of assessment of the necessity of each interest put forward by Meta IE, (2) the absence of a substantiated assessment regarding alternative advertising models that could be viable, (3) the incorrect finding in Meta IE Legitimate Interests Assessments that its behavioural advertising processing is unlikely to have an adverse impact on data subjects, and (4) the inappropriate reference to the fact that other businesses are also carrying out behavioural advertising, which does not have an impact on the lawfulness of such processing¹⁹⁹.

128. According to the settled case-law of the CJEU, when applying the necessity test, '*it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary*'²⁰⁰.

129. In its Bundeskartellamt Judgment, the CJEU also recalled that this second condition requires '*to ascertain that the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter*'²⁰¹. This condition must also be examined in conjunction with the principle of data minimisation under Article 5(1)(c) GDPR²⁰².

¹⁹⁶ IE SA Final Position Paper, paragraph 7.47, p. 17.

¹⁹⁷ Views of the NL SA of 4 May 2023 on Meta IE's choice of a new legal basis for the processing of personal data by Meta IE in the framework of Behavioural Advertising on its platforms Facebook and Instagram, paragraph 3.

¹⁹⁸ Views of IT SA on the IE SA FB Decision of 23 May 2023, p. 2, and views of IT SA on the IE SA IG Decision of 23 May 2023, p. 2.

¹⁹⁹ NO SA Order, p. 17-18.

²⁰⁰ Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:43, paragraph 30 and cited case-law; Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraph 28; Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 46.

²⁰¹ CJEU Bundeskartellamt Judgment, paragraph 108.

²⁰² CJEU Bundeskartellamt Judgment, paragraph 109.

130. In the EDPB Binding Decisions, the EDPB considered that there are realistic, less intrusive alternatives to behavioural advertising, making the processing at stake not ‘necessary’²⁰³.
131. In light of the above, the EDPB considers that there are grounds for concluding, as the IE SA did²⁰⁴, that Meta IE failed to fulfil the second condition of the ‘necessity test’ to be able to rely on Article 6(1)(f) GDPR for the processing of personal data collected on Meta’s products for purposes of behavioural advertising, in particular whether there are no other means that are less intrusive alternatives²⁰⁵ and regarding compliance with the principle of data minimisation under Article 5(1)(c) GDPR²⁰⁶.
132. The **third condition relates to the ‘balancing test’**.
133. In its Compliance Reports referring to the Meta IE Legitimate Interests Assessments, Meta IE has concluded that, in light of the ‘extensive measures and safeguards’ it implemented, the potential risks to data subjects identified are ‘appropriately mitigated’²⁰⁷.
134. More specifically, Meta IE refers *inter alia* to the following safeguards: the measures implemented to ensure transparency towards data subjects (e.g. through privacy policies and ‘Help center’ articles), the publication of advertising policies for users, the existence of restrictions on targeting criteria, the existence of control tools (in relation to advertising in general or to specific ads that are displayed to users)²⁰⁸, the possibility to object to the processing²⁰⁹ and the possibility to exercise data subjects’ data protection rights²¹⁰. Meta also argues that the language introduced to explain the change of legal basis and the impact on users, including their ability to object to the behavioural advertising processing at stake, ‘have been implemented to ensure that users have a reasonable expectation of Behavioural Advertising Processing and are aware of their right to object to this processing’²¹¹. In Meta IE’s Legitimate Interests Assessments, Meta further claims that ‘Users reasonably expect the processing of Platform Behavioural Information for behavioural advertising, taking into account the robust

²⁰³ EDPB Binding Decision 3/2022, paragraph 121 and the EDPB Binding Decision 4/2022, paragraph 124. As eluded to in the EDPB Binding Decisions, the AT SA, PL SA (only for EDPB Binding Decision 3/2022) and SE SAs mention as examples contextual advertising based on geography, language and content, which do not involve intrusive measures such as profiling and tracking of users. This analysis was made in the context of the legal basis of Art. 6(1)(b) GDPR.

²⁰⁴ IE SA Final Position Paper, paragraph 7.50, p. 18 and paragraph 6.3., p. 5.

²⁰⁵ IE SA Final Position Paper, paragraphs 7.46-7.48, p. 17.

²⁰⁶ IE SA Final Position Paper, paragraph 7.45, p. 16, and an analysis of the principle of data minimisation is included in paragraph 7.59, p. 19, with respect to the balancing test.

²⁰⁷ Meta IE Compliance Report on IE SA FB Decision, p. 10 and Meta IE Compliance Report on IE SA IG Decision, p. 11, both referring to sections 4 and in particular sections 4.2.b and 4.2.c of Meta IE Legitimate Interests Assessments.

²⁰⁸ Meta IE Legitimate Interests Assessments, of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision, section 4.2.c. on the implemented safeguards. Some safeguards are reiterated in Meta IE Compliance Report on IE SA FB Decision, p. 7-10 and Meta IE Compliance Report on IE SA IG Decision, p. 7-12.

²⁰⁹ Meta IE Legitimate Interests Assessments, of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision, section 4.2.e. on the opt-out tools.

²¹⁰ Meta IE Legitimate Interests Assessments, of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision, section 4.2.f. on data protection rights.

²¹¹ Meta IE Compliance Report on IE SA FB Decision, p. 7 and Meta IE Compliance Report on IE SA IG Decision, p. 7.

*transparency [Meta] has implemented (...), which contributes to managing user expectations around the Processing and personalised advertising more broadly*²¹².

135. In that regard, the EDPB notes that the IE SA concluded that, due to the failure to facilitate the right to object under Article 21 GDPR²¹³, the lack of any consideration of the right to private life (as enshrined in Article 7 of the Charter)²¹⁴ or data minimisation²¹⁵, and the insufficient consideration of the impact of the processing on the purpose limitation principle²¹⁶, Meta IE has not demonstrated that its legitimate interests in processing for behavioural advertising outweigh the fundamental rights and freedoms of data subjects²¹⁷. In particular regarding the right to object, the IE SA pointed out *inter alia* that '*there is no ability in these [objection] tools to turn off processing of data collected directly by [Meta IE] for advertising purposes, including content, audio, metadata about content, apps and features used, transactions, hashtag and the time, frequency and duration of activities on [Meta IE] products*' as these categories of data would still be used for the purpose of behavioural advertising according to Meta IE's privacy policy²¹⁸.
136. The IE SA also refers to a previous CJEU judgment of 24 September 2019, where the CJEU held that the data subjects' fundamental rights under Articles 7 and 8 of the Charter '*override, as a rule (...) the economic interest*' of a private operator²¹⁹.
137. The conclusion of the IE SA regarding the third condition was shared by a number of CSAs in their comments and reactions on the Meta IE Compliance Reports:
 - On 4 May 2023, the NL SA concluded that '*[t]he fundamental rights and freedoms of the data subject override the interest of [Meta IE] and the third parties involved*'²²⁰. The NL SA raised the following considerations:
 - '*some of the data processed by [Meta IE] for the purpose of behavioural advertising are special, sensitive kinds of personal data, which increase the weight attached to the interests of data subjects in the balancing act*'²²¹
 - '*Not only the type but also the sheer amount of data that is processed by a company with the size of [Meta IE] should be taken into account in the balancing act. For the purposes of behavioural advertisement, [Meta IE] processes a broad spectrum of (special) personal data from millions of users. These data are analysed and possibly stored, adjusted, and reused on a daily basis.*'²²²

²¹² Meta IE Legitimate Interests Assessments, of 3 April 2023, Annex 4 to Meta IE Compliance Report on IE SA FB Decision and Annex 4 to Meta IE Compliance Report on IE SA IG Decision, p. 7.

²¹³ IE SA Final Position Paper, paragraphs 7.60.-7.66., p. 19-21.

²¹⁴ IE SA Final Position Paper, paragraphs 7.57, p. 19.

²¹⁵ IE SA Final Position Paper, paragraph 7.59, p. 19.

²¹⁶ IE SA Final Position Paper, paragraph 7.58, p. 19.

²¹⁷ IE SA Final Position Paper, paragraph 7.67, p. 21, and paragraph 6.3., p. 5.

²¹⁸ IE SA Final Position Paper, paragraph 7.65., p. 20-21, referring in footnote 29 to p. 54-55 of Meta IE's privacy policy.

²¹⁹ IE SA Final Position Paper, paragraph 7.57., p. 19, referring to Judgment of the Court of Justice of the European Union of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraph 53. In this case, the private operator was a search engine. Also see case-law cited.

²²⁰ Views of the NL SA of 4 May 2023 on Meta IE's choice of a new legal basis for the processing of personal data by Meta IE in the framework of Behavioural Advertising on its platforms Facebook and Instagram, paragraph 3.

²²¹ Views of the NL SA of 14 May 2023, paragraph 43.

²²² Views of the NL SA of 14 May 2023, paragraph 44.

- ‘With regard to **user expectations**, the NL SA points out that, in line with the principle of accountability, the assessment of user expectations should take place **before** the processing is initiated under Art. 6(1)(f) GDPR. Controllers cannot simply “retroactively adjust” the expectations of existing users and bring processing in line with Art. 6(1)(f) GDPR, simply by providing them with some information – especially not when the essence of this information is hard to grasp.²²³’
 - ‘Furthermore, as also concluded by the EDPB in its decision 3/2022,²²⁴ the NL SA agrees with the EDPB that users do not sign up to [Meta IE]’s services to be served personalized content but for the sake of connecting with friends and family. Even in its changed Terms of Service, [Meta IE] presents its services as “services that enable people to connect with each other, build communities...”. The connection to people/friends/family is therefore still the service with which [Meta IE] seeks to attract new users. Even though “building businesses” is inserted as a third “goal” of the services of [Meta IE], this does not create the reasonable expectation that users’ personal data will be processed for the purpose of behavioural advertising’²²⁵.
 - ‘NL SA therefore concludes that users do not expect or should reasonably expect that their data are processed for the sake of behavioural advertising as done by [Meta IE].²²⁶
 - ‘Considering the **gravity of the risks identified**, NL SA finds that [Meta IE] indeed treads very lightly on these risks and their mitigation.²²⁶
 - ‘The NL SA therefore finds that the right to object as provided for in the GDPR, a core right when processing is undertaken on the basis of Art. 6(1)(f) GDPR, is therefore not properly respected by [Meta IE]²²⁷.
- On 12 May 2023, the ES SA identified the following shortcoming in Meta IE’s assessment of the balancing test:
 - ‘Regarding the **impact on data subjects**, it is not established that it does not concern sensitive data.
 - As regards the **way in which data is processed**, data is processed massively, comprehensively and in combination with all types of data obtained from other sources, without taking into account the principle of data minimization.
 - As regards the **data subject’s reasonable expectations**, the data typology reflected in the privacy policy is not easily understandable to the average user, who does not know exactly what data is being processed and what the extent of such processing is. In order for the user to know what type of data is being processed and how they are being processed, the user must also look up several documents.
 - As regards the **position of the controller and the data subject**, there is no balance of power, Meta [IE] is a large company which imposes its conditions on its users without they have the possibility of choosing or not certain processing operations and which of

²²³ Views of the NL SA of 14 May 2023, paragraph 45.

²²⁴ Views of the NL SA of 14 May 2023, paragraph 46.

²²⁵ Views of the NL SA of 14 May 2023, paragraph 49.

²²⁶ Views of the NL SA of 14 May 2023, paragraph 51.

²²⁷ Views of the NL SA of 14 May 2023, paragraph 63.

their data are processed. There is also no analysis of how the [processing] affects vulnerable sectors, and how to mitigate possible negative effects.

- *Finally, with regard to the **additional safeguards** included to prevent undue impact on data subjects, as already stated, the principle of data minimization is not taken into account, there is no indication of what actions [Meta IE] takes to prevent the processing of sensitive data indirectly and, as explained below, the GDPR is not complied with regard to the right to object.²²⁸ [emphasis added in bold]*
 - On 15 May 2023, the FI SA stated that '*[Meta IE]’s legal interests assessment (...) seems to be rather one-sided and superficial and fails to convince why the interests of [Meta IE] or third parties should override the interests and fundamental rights of the data subjects*'²²⁹.
 - On 23 May 2023, the IT SA notes in relation to Meta IE Legitimate Interests Assessments that '*it is as if the controller were shifting the burden of proof regarding legitimate interest as the legal basis of processing on the data subjects – who conversely should be called into play as key actors in the two subsequent steps of the legitimate interest test, i.e. when assessing the necessity of the processing and performing the required balancing exercise*'²³⁰.
 - In the NO SA Order, the NO SA rejects Meta IE's assumption that the data subjects undisputedly want and expect behavioural advertising based on monitoring and profiling of their behaviour²³¹. Therefore, according to the NO SA, Meta IE's assessment of the elements of Article 6(1)(f) GDPR has been skewed²³². In addition, the NO SA refers to the paragraph 117 of the CJEU Bundeskartellamt Judgment, which held that '*data subjects cannot reasonably expect that the operator of the social network will process that user’s personal data, without his or her consent, for the purposes of personalised advertising*'²³³. Further, the NO SA considers that informing data subjects about behavioural advertising processing does not mean that it falls within their reasonable expectations and in any case, data subjects are not realistically able to read the privacy policies of every service used, including Meta IE's privacy policies²³⁴. The NO SA also argues that Meta IE fails to show that Meta IE's interests outweigh the rights and freedoms of data subjects²³⁵.
138. The IE SA made an overall conclusion on the three-step test²³⁶ that Meta IE has not demonstrated compliance with Article 6(1)(f) GDPR for the processing at stake²³⁷. The IE SA highlighted, both in the IE SA Provisional Position Paper and IE SA Final Position Paper that this conclusion stems from the following reasons: (1) '*[Meta IE] has not made out that the processing is necessary for legitimate interests. Its explanations of the impact of the processing on its business are too vague to allow the [IE*

²²⁸ Views of the ES SA of 12 May 2023, p. 5.

²²⁹ Views of the FI SA of 15 May 2023, preliminary remarks on Meta’s new legal basis in relation to the processing of personal data for the purposes of behavioural advertising in Facebook and Instagram services, p. 2.

²³⁰ Views of IT SA on the legal basis order and transparency order relating to the IE SA FB Decision, p. 2, and views of IT SA on the legal basis order and transparency order relating to the IE SA IG Decision of 23 May 2023, p. 2.

²³¹ NO SA Order, p. 15-16.

²³² NO SA Order, p. 15-16.

²³³ NO SA Order, p. 17.

²³⁴ NO SA Order, p. 16.

²³⁵ NO SA Order, p. 17-23.

²³⁶ IE SA Final Position Paper, paragraphs 7.27-7.28, p. 12-13, referring to the CJEU Bundeskartellamt Judgment, paragraph 126.

²³⁷ IE SA Final Position Paper, paragraph 7.30, p. 13.

SA] to determine that there is no less intrusive alternative that can be pursued', (2) '[Meta IE] has not demonstrated that the balancing favours its processing. In particular, the opt-out mechanism provided does not comply with the GDPR'²³⁸. The conclusions of the IE SA regarding the results of the three-step test was shared by a number of CSAs, which also raised the inappropriate reliance by Meta IE to Article 6(1)(f) GDPR:

- On 18 April 2023, the AT SA stated that processing operations in connection with '*behavioural advertising processing*' cannot be based on Article 6(1)(f) GDPR²³⁹.
- On 12 May 2023, the ES SA indicated that Meta IE Legitimate Interests Assessments '*did not demonstrate that the processing carried out by Meta IE with the purpose of behavioural advertisement can be based on [A]rticle 6(1)(f) [GDPR] since it does not meet the requirements of this article*'²⁴⁰.
- In the NL SA Mutual Assistance Request sent on 30 May 2023, the NL SA expressed concerns as to Meta IE's reliance on Article 6(1)(f) GDPR, taking into account '*the fact that the controller could not have been unaware of already established guidance from the EDPB, nor of the position of several CSAs on the matter, but chose to explore the path of Article 6(1)(f) [GDPR] regardless*'²⁴¹. The NL SA states that '*Meta [IE] cannot invoke Article 6(1)(f) [GDPR] as a valid legal basis to process the personal data of its users for the purposes of behavioural advertising*', and that this conclusion is '*in line with several EDPB and WP29 Guidance documents, which underpin that the appropriateness of using Article 6(1)(f) [GDPR] as a legal basis for the processing concerned is highly questionable*'²⁴².

139. In previous judgments, the CJEU clarified that when carrying out the 'balancing test', the data controller '*must take account of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter*'²⁴³.

140. In its Bundeskartellamt Judgment, the CJEU held the following obiter dictum:

*'as can be seen from recital 47 of the GDPR, the interests and fundamental rights of the data subject may in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing'*²⁴⁴.

*'(...) such processing must also be necessary in order to achieve that interest and the interests or fundamental freedoms and rights of the data subject must not override that interest. In the context of that balancing of the opposing rights at issue, namely, those of the controller, on the one hand, and those of the data subject, on the other, account must be taken, as has been noted (...) above, in particular of the reasonable expectations of the data subject as well as the scale of the processing at issue and its impact on that person.'*²⁴⁵

²³⁸ IE SA Final Position Paper, paragraph 6.3, p. 5 ; IE SA Provisional Position Paper, paragraph 5.3, p. 4 (in slightly different terms).

²³⁹ IMI report on Compliance in the Facebook case.

²⁴⁰ Views of the ES SA, 12 May 2023, p. 6.

²⁴¹ NL SA Mutual Assistance Request, p. 2.

²⁴² NL SA Mutual Assistance Request, p. 1, where a reference is made to the EDPB Guidelines 8/2020 on the targeting of social media users.

²⁴⁴ CJEU Bundeskartellamt Judgment, paragraph 112.

²⁴⁴ CJEU Bundeskartellamt Judgment, paragraph 112.

²⁴⁵ CJEU Bundeskartellamt Judgment, paragraph 116.

*'In this regard, it is important to note that, despite the fact that the services of an online social network such as Facebook are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising. In those circumstances, it must be held that the interests and fundamental rights of such a user override the interest of that operator in such personalised advertising by which it finances its activity, with the result that the processing by that operator for such purposes cannot fall within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR.'*²⁴⁶ [emphasis added]

141. In the IE SA Provisional Position Paper issued before the CJEU Bundeskartellamt Judgment, the IE SA provisionally found that Meta IE had not demonstrated compliance with Article 6(1)(f) GDPR²⁴⁷ as Meta IE had not demonstrated that it could rely on Article 6(1)(f) GDPR²⁴⁸. The IE SA then confirmed that Meta IE has not demonstrated compliance with Article 6(1)(f) GDPR following the analysis of the CJEU Bundeskartellamt Judgment as it states in its Final Position Paper that '*Prior to the date of [the Bundeskartellamt] judgment, the [IE SA] had analysed [Meta IE]’s reliance on Article 6(1)(f) [GDPR] and had come to the provisional conclusion that [Meta IE] had not demonstrated compliance with that provision*' and that '*the CJEU indicated that there are significant barriers to [Meta IE] seeking to rely on Article 6(1)(f) [GDPR] for the behavioural advertising processing at issue in that judgment*'²⁴⁹.
142. The EDPB notes Meta IE’s arguments regarding the alleged irrelevance of the CJEU Bundeskartellamt Judgment²⁵⁰. Meta considers that this judgment ‘*does not rule out Article 6(1)(f) [GDPR] “as a matter of principle” as a valid legal basis for [Meta IE]’s Behavioral Advertising Processing. The judgment assessed Article 6(1)(f) [GDPR] (and the element of “necessity”) in the context of different processing than is at-issue here (i.e., data collected off-[Meta])²⁵¹, and to a limited extent cross-product data processing, as opposed to data collected on-[Meta] products*. (...) Further, the CJEU did not (and could not as a matter of law) issue a blanket finding that users’ interests will always outweigh [Meta IE]’s and third parties’ legitimate interests in the context of personalised advertising (...)²⁵².
143. As regards the scope of the CJEU Bundeskartellamt Judgment, the EDPB notes the references made to data collection from other services of the group to which an operator belongs²⁵³.

²⁴⁶ CJEU Bundeskartellamt Judgment, paragraph 117.

²⁴⁷ IE SA Provisional Position Paper, paragraph 6.26, p. 11.

²⁴⁸ IE SA Provisional Position Paper, paragraph 5.3, p. 4.

²⁴⁹ IE SA Final Position Paper, paragraph 7.26, p. 12.

²⁵⁰ Meta IE’s Response to IE SA’s Provisional Position Paper of 4 August 2023, section 1.5 (A). See also ENG Version of Meta IE Merits Complaint submitted to the Oslo District Court of 16 October 2023 (corrected), p. 38 and Meta IE’s Submissions of 26 September 2023, p. 10-11.

²⁵¹ Data collected ‘off’-Meta products refers data collected outside of Meta’s products, such as on third-party websites, apps and certain offline interactions (e.g., purchases).

²⁵² Meta IE’s Response to IE SA’s Provisional Position Paper of 4 August 2023, section 1.5 (A) and section 2 for a more detailed analysis of the CJEU Bundeskartellamt Judgment.

²⁵³ In that regard, paragraph 86 of the CJEU Bundeskartellamt Judgment states: ‘*By Questions 3 and 4, which it is appropriate to examine together, the referring court asks, in essence, whether and under what conditions points (b) and (f) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of such data, may be considered to be necessary for the performance of a contract to which the data subjects are party, within the meaning of point (b), or for the purposes of the legitimate interests pursued by the controller or*

144. The EDPB acknowledges that the behavioural advertising processing that Meta carries out in reliance of Article 6(1)(f) GDPR and that is examined for the purpose of this section 4.1.1.3²⁵⁴ relates to personal data collected on Meta's products while, according to Meta IE, the CJEU Bundeskartellamt Judgment mostly relates to personal data obtained from third party advertising partners outside of Meta's products. However, the EDPB considers that this Judgment, addressed to Meta IE, Meta Platforms Inc. and Facebook Deutschland GmbH²⁵⁵, outlines the way the balancing exercise may be carried out for the purpose of behavioural advertising, which is also relevant for personal data collected on Meta's products.
145. The EDPB recalls its previous guidelines where it highlighted that '*it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering.*'²⁵⁶
146. The EDPB considers that this guidance is relevant for the processing at stake carried out by Meta IE, which, as provided in the EDPB Binding Decisions, is intrusive given its scale and the extensive amounts of data that is processed by Meta IE²⁵⁷. In those decisions, the EDPB outlined '*the complexity, massive scale and intrusiveness of the behavioural advertising practice that Meta IE conducts through the Facebook [or Instagram] service*'²⁵⁸. In other words, '*[b]ehavioural advertising, as briefly described in [paragraph 95 of the EDPB Binding Decision 3/2022 and paragraph 98 of the Binding Decision 4/2022]*²⁵⁹ *is a set of processing operations of personal data of great technical complexity, which has a*

by a third party, within the meaning of point (f). That court asks, in particular, whether, to that end, certain interests which it explicitly lists constitute 'legitimate interests' within the meaning of the latter provision.'

²⁵⁴ Meta IE indicates to rely on Art. 6(1)(a) GDPR to process personal data obtained by Meta IE from third party advertising partners. Such data is about users' activity off-Meta's products. See footnotes 89 and 149 above in that regard.

²⁵⁵ The request for a preliminary ruling in the CJEU Bundeskartellamt Judgment has been made in proceedings between Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, and Facebook Deutschland GmbH, on the one hand, and the Bundeskartellamt. Meta IE operates the online social network Facebook in the EU. See CJEU Bundeskartellamt Judgment, paragraphs 2 and 26.

²⁵⁶ Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018, endorsed by the EDPB on 25 May 2018, p. 15. This was referred to by the NO SA in the NO SA Order, p. 9. This same statement was reiterated by the EDPB in the EDPB Guidelines on the targeting of social media users, Version 2.0, adopted on 13 April 2021, paragraph 56.

²⁵⁷ EDPB Binding Decision 3/2022, paragraph 444 and EDPB Binding Decision 4/2022, paragraph 413.

²⁵⁸ EDPB Binding Decision 3/2022, paragraph 96 and the EDPB Binding Decision 4/2022, paragraph 99.

²⁵⁹ Paragraph 95 of EDPB Binding Decision 3/2022 states: '*These requests for preliminary rulings mention that [Meta IE] collects data on its individual users and their activities on and off its Facebook social network service via numerous means such as the service itself, other services of the Meta group including Instagram, WhatsApp and Oculus, third party websites and apps via integrated programming interfaces such as Facebook Business Tools or via cookies, social plug-ins, pixels and comparable technologies placed on the internet user's computer or mobile device. According to the descriptions provided, [Meta IE] links these data with the user's Facebook account to enable advertisers to tailor their advertising to Facebook's individual users based on their consumer behaviour, interests, purchasing power and personal situation. This may also include the user's physical location to display content relevant to the user's location. Meta IE offers its services to its users free of charge and generates revenue through this personalised advertising that targets them, in addition to static advertising that is displayed to every user in the same way.'*

Paragraph 98 of EDPB Binding Decision 4/2022 states: '*These requests for preliminary rulings mention that Meta IE collects data on its individual users and their activities on and off its Facebook service via numerous means such as the service itself, other services of the Meta group including Instagram, WhatsApp and Oculus, third party websites and apps via integrated programming interfaces such as Facebook Business Tools or via cookies, social*

*particularly massive and intrusive nature*²⁶⁰. The IE SA reiterated this conclusion in the IE SA Decisions: ‘*It is therefore clear that the Board considers (...) the nature and scope of the processing to be extensive, complex, intrusive and on a massive scale*’²⁶¹.

147. In light of the above and taking into account the legal analysis provided by the IE SA (see for example in paragraphs 135 and 138 above, as supported by the assessment performed by the of the CSAs), the EDPB considers that the interests and fundamental rights of data subjects override the legitimate interests put forward by Meta IE for the processing of personal data collected on Meta’s products for the purposes of behavioural advertising, with the result that Meta IE did not fulfil the third condition of Article 6(1)(f) GDPR.
148. In light of the above analysis of the EDPB from paragraph 111 to 147, the EDPB considers that Meta IE inappropriately relies on Article 6(1)(f) GDPR to process personal data collected on its products for the purpose of behavioural advertising.

4.1.1.3.4 Conclusion as to the infringement of Article 6(1) GDPR

149. The compliance approach adopted by Meta IE has been assessed in the IE SA Final Position Paper as follows:
 - Meta IE seeks to still rely on Article 6(1)(b) GDPR to process some specific categories of personal data²⁶², for advertising purposes²⁶³;
 - Meta IE seeks to rely on Article 6(1)(f) GDPR to process other personal data for the purposes of behavioural advertising²⁶⁴ - solely for personal data collected on Meta’s products²⁶⁵;
 - Meta IE relies on Article 6(1)(a) GDPR to process personal data provided to Meta IE by third party advertising partners²⁶⁶.
150. Meta IE [REDACTED] is willing to rely on Article 6(1)(a) GDPR as its legal basis [REDACTED] through the Meta IE’s Consent Proposal²⁶⁷.
151. The EDPB highlights the need to assess the compliance of the processing activities within the scope of the IE SA Decisions with Article 6(1) GDPR at this point in time. [REDACTED]

*plug-ins, pixels and comparable technologies placed on the internet user’s computer or mobile device*¹⁶⁴. According to the descriptions provided, Meta IE links these data with the user’s Facebook account to enable advertisers to tailor their advertising to Facebook’s individual users based on their consumer behaviour, interests, purchasing power and personal situation. This may also include the user’s physical location to display content relevant to the user’s location. Meta IE offers its services to its users free of charge and generates revenue through this personalised advertising that targets them, in addition to static advertising that is displayed to every user in the same way.’

²⁶⁰ EDPB Binding Decision 3/2022, paragraph 123 and the EDPB Binding Decision 4/2022, paragraph 126.

²⁶¹ IE SA FB Decision, paragraph 9.23 and IE SA IG Decision, paragraph 243.

²⁶² See paragraph 91 above.

²⁶³ IE Final Position Paper, paragraphs 6.2 and 7.1-7.22.

²⁶⁴ IE Final Position Paper, paragraphs 6.3 and 7.23-7.67.

²⁶⁵ IE Final Position Paper, paragraph 7.23, referring to Meta IE’s Letter to the IE SA of 30 June 2023.

²⁶⁶ IE SA Final Position Paper, paragraph 7.23, referring to Meta IE’s Letter to the IE SA of 30 June 2023.

²⁶⁷ Letter from Meta IE to IE SA regarding consent of 27 July 2023, p. 2.

[REDACTED]²⁶⁸. For the sake of clarity, the EDPB specifies that Meta IE's Consent Proposal was not assessed in its merits for the purposes of this urgent binding decision. In this regard, the EDPB may only take note of the existence of an ongoing evaluation of the Meta IE's Consent Proposal by the IE SA and the CSAs.

152. According to the EDPB, there is an ongoing infringement of Article 6(1) GDPR arising from inappropriate reliance on Article 6(1)(b) GDPR for processing of personal data, including location data and advertisement interaction data collected, on Meta's products for behavioural advertising purposes²⁶⁹.
153. In addition, the EDPB concludes that there is an ongoing infringement of Article 6(1) GDPR arising from inappropriate reliance on Article 6(1)(f) GDPR for processing personal data collected on Meta's products for behavioural advertising purposes²⁷⁰.

4.1.2 On the infringement of the duty to comply with decisions by supervisory authorities

4.1.2.1 Summary of the overall position of the NO SA

154. According to the NO SA, since the deadline for complying with the IE SA Decisions was 5 April 2023 but the infringement of Article 6(1) GDPR still persists more than six months later, Meta IE failed to ensure compliance with the IE SA Decisions, and hence infringed its duty to comply with the SAs' decisions²⁷¹. The NO states further that there is consensus on the European level between the IE SA and the CSAs that the processing continues to be unlawful²⁷², and that '*as acknowledged by the IE SA itself, Meta IE has failed to ensure compliance with [the IE SA Decisions]*'²⁷³. The NO SA stated that this non-compliance constitutes in itself an independent violation of the GDPR²⁷⁴ for which Article 83(5)(e) GDPR envisages a fine which may be imposed in addition to the fines imposed by the IE SA Decisions²⁷⁵.

4.1.2.2 Summary of the position of the controller

155. Meta IE stated that, prior to the IE SA Decisions, it relied on Article 6(1)(b) GDPR in a good faith manner and its '*bona fide belief that it was lawful for it to do so*'²⁷⁶.
156. Following to the IE SA Decisions, Meta IE argued that it took substantial steps to bring its processing activities into '*what it believes was compliance with [the IE SA] decisions*'²⁷⁷, including by changing its legal basis from Article 6(1)(b) GDPR to Article 6(1)(f) GDPR for the processing of personal data collected on its products for the purposes of behavioural advertising²⁷⁸.

²⁶⁸ [REDACTED]

²⁶⁹ See the analysis carried out above in Section 4.1.1.2.3 and paragraphs 98-99.

²⁷⁰ See the analysis carried out above in Section 4.1.1.3.3 and paragraph 148.

²⁷¹ NO SA Request to the EDPB, p. 6.

²⁷² NO SA Request to the EDPB, p.12.

²⁷³ NO SA Request to the EDPB, p. 6.

²⁷⁴ NO SA Request to the EDPB, p. 6 and Letter from the NO SA to the IE SA dated 11 October 2023, p. 2.

²⁷⁵ NO SA Request to the EDPB, p. 6.

²⁷⁶ Letter from Meta IE to NO SA of 4 August 2023, in relation to right to be heard, paragraph 65.

²⁷⁷ Letter from Meta IE to NO SA of 4 August 2023, in relation to the right to be heard, dated paragraph 65.

²⁷⁸ Meta IE's Compliance Report regarding the Facebook Service (IN-18-5-5) of 3 April 2023 (hereinafter, '**Compliance Report on IE SA FB Decision**'), paragraph 2.1 and Meta IE's Compliance Report regarding the Instagram Service (IN-18-5-7) of 3 April 2023 (hereinafter, '**Compliance Report on IE SA IG Decision**'), paragraph 2.1 (together, the '**Compliance Reports**').

157. Meta IE takes the view that neither the EDPB Binding Decisions nor the IE SA Decisions ordered Meta IE to rely on a specific legal basis for the processing of personal data collected on its products for behavioural advertising purpose under Article 6(1) GDPR, such as Article 6(1)(a) GDPR²⁷⁹. As a result, Meta IE still currently seeks to rely on Article 6(1)(b) GDPR to process some specific categories of personal data that it does not consider to be behavioural data²⁸⁰, and on Article 6(1)(f) GDPR to process other personal data for the purposes of behavioural advertising²⁸¹ - solely for personal data collected on its products²⁸².
158. After considering the IE SA Provisional Position Paper (including the IE SA's interpretation of the CJEU Bundeskartellamt Judgment), Meta IE stated that it was willing to implement the necessary measures to rely on Article 6(1)(a) GDPR as its legal basis for processing for the purpose of behavioural advertising through the Meta IE's Consent Proposal²⁸³.
159. After considering the IE SA's Final Position Paper, Meta IE stated that it considered itself as compliant with the IE SA Decisions [REDACTED]

²⁸⁴ [REDACTED]

²⁸⁵ [REDACTED]

4.1.2.3 Analysis of the EDPB

160. The EDPB recalls that Article 60(10) GDPR provides for the duty for the controller to '*take the necessary measures to ensure compliance with the decision [taken in the context of the cooperation mechanism] as regards processing activities in the context of all its establishments in the Union*'²⁸⁶.
161. The EDPB also recalls that non-compliance with an order of an SA pursuant to Article 58(2) GDPR constitutes an infringement that may be sanctioned by way of an administrative fine pursuant to Article 83(5)(e) GDPR and Article 83(6) GDPR²⁸⁷.

²⁷⁹ Meta IE's Submissions of 26 September 2023, p. 10, and Meta IE's Submissions of 25 August 2023, p. 4 and 16.

²⁸⁰ See paragraph 91 above and the IE SA Final Position Paper, paragraphs 6.2 and 7.1-7.22.

²⁸¹ IE SA Final Position Paper, paragraphs 6.3 and 7.23-7.67.

²⁸² See paragraph 104 above and the IE SA Final Position Paper, paragraph 7.23, referring to Meta IE's Letter to the IE SA of 30 June 2023.

²⁸³ Letter from Meta IE to IE SA regarding consent of 27 July 2023, p. 2.

²⁸⁴ Meta IE' Submissions of 25 August 2023, paragraph 61.

²⁸⁵ Meta IE's Submissions of 25 August 2023, paragraph 64.

²⁸⁶ Article 60 GDPR.

²⁸⁷ According to Art. 83(5)(e) GDPR, '*non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) [GDPR] or failure to provide access in violation of Article 58(1) [GDPR]*' is an infringement that '*shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*'. Art. 83(6) GDPR provides: '*Non-compliance with an order by the supervisory authority as referred to in Article 58(2) [GDPR] shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*'.

162. The EDPB confirms, in line with the view of the NO SA²⁸⁸, that non-compliance with decisions of supervisory authorities is in itself an independent violation of the GDPR²⁸⁹.
163. As already noted above, the IE SA Decisions required Meta IE to, *inter alia*, take the necessary action to address the finding that Meta IE is not entitled to process personal data for behavioural advertising on the basis of Article 6(1)(b) GDPR and to bring its processing of personal data for behavioural advertising purposes into compliance with Article 6(1) GDPR.²⁹⁰ Also, the IE SA made clear that the actions Meta IE should take to comply with the IE SA Decisions may include, but were not limited to, the identification of an appropriate alternative legal basis in Article 6(1) GDPR²⁹¹ and may include the implementation of any necessary measures required to satisfy the conditionality associated with that/those alternative legal basis/bases²⁹². The deadline for compliance with the IE SA Decisions was 5 April 2023.

The EDPB notes that in the IE SA Final Position Paper, the IE SA found that Meta IE failed to demonstrate compliance with the IE SA Decisions, and states that Meta IE '*failed to demonstrate that it no longer relies on Article 6(1)(b) GDPR to process personal data for behavioural advertising*' and '*failed to demonstrate that it has a lawful basis to process Platform behavioural Data for behavioural advertising*'²⁹³.

164. The EDPB notes that the NL SA also stated that '*As Meta [IE] has publicly stated that it already makes use of Article 6(1)(f) [GDPR] as a legal basis, this conclusion means that - at the moment - personal data of millions of European data subjects are being processed without there being a valid legal basis. This moreover means that Meta [IE] does not comply with the [IE SA]’s order in the [IE SA Decisions] to bring these processing operations in line with Article 6 GDPR*'.²⁹⁴
165. The EDPB notes the view of the IE SA that neither the GDPR nor Irish national law prescribes the manner in which the assessment of the steps taken by the controller in purported compliance with the orders of an SA should be carried out²⁹⁵. In this respect, the EDPB notes that Meta IE does not contest that the IE SA’s findings made subsequently to the IE SA Decisions are made '*to implement the existing [IE SA] decisions pursuant to Article 60(10) GDPR*'.²⁹⁶
166. In respect of Meta IE’s argument that it fully complied with the IE SA Decisions by taking, first, substantial steps to bring its processing activities into compliance by 5 April 2023²⁹⁷ and, secondly, steps in the direction of the Meta IE’s Consent Proposal²⁹⁸, the EDPB highlights that these elements do

²⁸⁸ Letter from the NO SA to the IE SA of 17 September 2023 in relation to the right to be heard, p. 7.

²⁸⁹ ‘*Non-compliance with a corrective power previously ordered may be considered either as an aggravating factor, or as a different infringement in itself, pursuant to Art. 83(5)(e) and Art. 83(6) GDPR. Therefore, due note should be taken that the same non-compliant behaviour cannot lead to a situation where it is punished twice*’, EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, version 2.1, paragraph 103.

²⁹⁰ See IE SA FB Decision, paragraph 10.44b; IE SA IG Decision, paragraph 212.

²⁹¹ IE SA FB Decision, paragraph 10.44b and IE SA IG Decision, paragraph 10.

²⁹² IE SA FB Decision, paragraph 8; and IE SA IG Decision, paragraph 212.

²⁹³ IE SA Final Position Paper, section 8, p. 25. In relation to Meta IE’s reliance on Article 6(1)(b) GDPR, also see paragraphs 96-99 above. In relation to Meta IE’s reliance on Art. 6(1)(f) GDPR, also see paragraphs 121, 135, 138 above.

²⁹⁴ NL SA Mutual Assistance Request, p. 2.

²⁹⁵ Letter of the IE SA to Meta IE of 14 June 2023, p. 1-2.

²⁹⁶ Meta IE’s Submissions of 26 September 2023, p. 12 and 13.

²⁹⁷ Meta IE’s Submissions of 26 September 2023, p. 10 and Meta IE’s Submissions of 16 October 2023, p. 5. See also Meta IE’s Submissions of 25 August 2023, p. 33.

²⁹⁸ Letter from Meta IE to IE SA regarding consent of 27 July 2023, p. 2.

not in themselves contradict the conclusion that at this point in time compliance with Article 6(1) GDPR for the processing activities within the scope of the IE SA Decisions has not yet been achieved while the deadline to implement the IE SA Decisions was 5 April 2023.

4.1.2.4 Conclusion as to the infringement of the duty to comply with decisions by supervisory authorities

167. In light of its findings that Meta IE still relies inappropriately on Article 6(1)(b) GDPR to process personal data, including location data and advertisement interaction data, collected on its products for the purpose of behavioural advertising³⁰⁰ and on Article 6(1)(f) GDPR to process personal data collected on its products for the purpose of behavioural advertising³⁰¹ the EDPB finds, in line with the conclusions drawn by the IE SA³⁰² and with the views expressed in particular by the NO SA³⁰³ [REDACTED]³⁰⁴ in the course of the proceedings, that Meta IE did not achieve compliance with the IE SA Decisions within the deadline for compliance and is therefore currently in breach of its duty to comply with decisions by supervisory authorities.

4.2 On the existence of urgency to adopt final measures by way of derogation from the cooperation and consistency mechanisms

168. The second element to assess pursuant to Article 66(2) GDPR is the existence of an urgency situation justifying a derogation from the regular cooperation procedure.
169. The urgent intervention of the EDPB pursuant to Article 66(2) GDPR is exceptional, and derogates from the general rules applicable to the regular consistency and cooperation mechanisms.
170. Considering the fact that the urgency procedure under Article 66(2) GDPR is a derogation to the standard consistency and cooperation mechanisms, it must be interpreted restrictively. Therefore, the EDPB may request final measures under Article 66(2) GDPR only if the regular cooperation or consistency mechanisms cannot be applied in their usual manner, due to the urgency of the situation³⁰⁵.
171. In addition, Article 61(8) GDPR provides that, where an SA does not provide the information referred to in Article 61(5) GDPR within one month of receiving a mutual assistance request from another SA, the '*urgent need to act under Article 66(1) [GDPR] shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2) [GDPR]*'. If such a presumption applies, the urgent nature of an Article 66(2) request for an urgent binding decision can be presumed and does not need to be demonstrated³⁰⁶.

²⁹⁹ Letter from NO SA to Meta IE and Facebook Norway of 17 September 2023 in relation to the right to be heard, p. 9.

³⁰⁰ See paragraphs 98-99, and 152 above.

³⁰¹ See paragraphs 148 and 153 above.

³⁰² IE SA Final Position Paper, section 8, p. 25.

³⁰³ NO SA Request to the EDPB, p. 6.

³⁰⁴ [REDACTED]

³⁰⁵ EDPB Urgent Binding Decision 01/2021, adopted on 12 July 2021, paragraph 167.

³⁰⁶ EDPB Urgent Binding Decision 01/2021, adopted on 12 July 2021, paragraph 170.

172. In the present procedure, the NO SA requested the EDPB to adopt a decision pursuant to Article 66(2) GDPR, in order to urgently request the IE SA to impose final measures on Meta IE. The request has been made following to the adoption of provisional measures pursuant to Article 66(1) GDPR³⁰⁷ which are only applicable in Norway, and are only valid for three months.
173. In the sections below, the EDPB analyses first whether the circumstances of the present case demonstrate the existence of urgency and the need to derogate from the cooperation and consistency mechanisms (section 4.2.1 below) before analysing whether the presumption described in Article 61(8) GDPR is applicable to the circumstances of the case (section 4.2.2).

4.2.1 On the existence of urgency and the need to derogate from the cooperation and consistency mechanisms

4.2.1.1 Summary of the position of the NO SA

174. The NO SA considers that ‘Regardless of the applicability of the Article 61(8) presumption, in the present case there is an urgent need for a binding decision from the EDPB in accordance with Article 66(2) GDPR, in order to protect the rights and freedoms of data subjects’³⁰⁸.
175. According to the NO SA, the processing in question is detrimental to individuals’ fundamental rights, and failing to put an end to this processing would thus expose these data subjects to a risk of serious and irreparable harm³⁰⁹. In more details, the NO SA takes the view that:
- The infringements have been occurring for a significant amount of time and are of an especially serious nature, as they have a considerable impact on the users of Meta’s products whose online activities are *‘constantly, intrusively and opaquely monitored and profiled by Meta’*, which *‘may give rise to the feeling that their private life is being continuously surveilled’*.³¹⁰
 - The infringements affect over 250 million average monthly active users in the EU, including vulnerable data subjects in need of particular protection, such as minors, elderly people and people with cognitive disabilities³¹¹.
 - The filtering of the specific ads that are displayed on Facebook or Instagram has an adverse effect on data subjects’ freedom of information and on political participation³¹² while creating *‘a potential for reinforcement of existing stereotypes, and it can leave data subjects open to discrimination’*³¹³.
 - Not taking urgent action to ensure compliance with the IE SA Decisions would deprive data subjects of the right to seek an effective remedy against a data controller from SAs under Article 77 GDPR³¹⁴.

³⁰⁷ Art. 66(4) GDPR; as described in Section 2.1 above.

³⁰⁸ NO SA Request to the EDPB, p. 10.

³⁰⁹ NO SA Request to the EDPB, p. 10.

³¹⁰ NO SA Request to the EDPB, p. 10, referring to CJEU Bundeskartellamt Judgment, paragraph 118.

³¹¹ NO SA Request to the EDPB, p. 10.

³¹² NO SA Order, p. 22.

³¹³ NO SA Request to the EDPB, p. 10; NO SA Order, p. 22.

³¹⁴ NO SA Order, p. 28.

- The NO SA is of the view that there is no measure that could be applied retroactively to repair the violation of the rights and freedoms of data subjects³¹⁵.
176. In addition, the NO SA states that there has been a '*continued refrainment from enforcement*' on the part of the IE SA³¹⁶. The NO SA takes the view that despite the fact that infringements are taking place appears uncontroversial among supervisory authorities, '*the IE SA appears to be unwilling to demand that such infringements be ceased without any further delays*'³¹⁷. In this respect, the NO SA states that the failure to firmly and expediently react to non-compliance with the IE SA Decisions not only deprives data subjects of the protection they are entitled to, but is also contrary to supervisory authorities' duty to ensure that the GDPR is respected in practice³¹⁸.
177. More generally, in the view of the NO SA, not reacting to Meta IE's prolonged state of non-compliance would set a dangerous precedent³¹⁹ as it would '*invite dilatory strategies from non-compliant controllers*' and undermine the authority of the IE SA, the CSAs and the EDPB³²⁰. For the NO SA, a failure to adopt the requested urgent binding decision in the present circumstances would entail serious risks that the Article 66 GDPR mechanism would turn in to a '*paper tiger*'³²¹.
178. The NO SA argues that an EDPB urgent binding decision would be a narrow and strictly limited exception to the primacy of the LSA in ensuring compliance with an Article 60 GDPR decision and would not set a precedent for derogating from the standard one-stop-shop cooperation procedure³²² as it would be issued after the completion of an Article 60 GDPR process, following the adoption by the IE SA of the IE SA Decisions³²³ and given the fact that the IE SA does not envisage to start a new Article 60 GDPR procedure³²⁴.
179. Further, the NO SA argues that final measures would not interfere with [REDACTED] commitment to change the legal basis for behavioural advertising to consent³²⁵. According to the NO SA, '*if Meta [IE] would be ordered to stop all such processing activities based on Article 6(1)(b) [GDPR] and [Article 6(1)] (f) pending the identification of a valid legal basis, it would have an incentive to expeditiously identify adequate and lawful solutions to resume its processing activities as soon as possible*'³²⁶.
180. [REDACTED]

³¹⁵ NO SA Rejection of Meta IE and Facebook Norway's Request for Deferred Implementation of the Order dated 7 August 2023, p. 1.

³¹⁶ NO SA Order, p. 12.

³¹⁷ NO SA Request to the EDPB, p. 6.

³¹⁸ NO SA Request to the EDPB, p. 6.

³¹⁹ Letter of NO SA to IE SA of 11 October 2023, p. 11.

³²⁰ NO SA Order, p. 28; NO SA Request NO SA Request to the EDPB, p. 12.

³²¹ NO SA Request to the EDPB, p. 12, referring to the opinion of Advocate General Bobek in Case C-645/19, Facebook Ireland and Others, paragraph 119 and paragraph 122.

³²² NO SA Request to the EDPB, p. 12.

³²³ NO SA Request to the EDPB, p. 10-11, referring to IE SA Information on Procedure (response to SE SA) of 4 May 2023 where the IE SA had indicated via the IE SA IMI Informal Consultations that they would '*not be preparing any further decision in this matter*'.

³²⁴ NO SA Request to the EDPB, p. 11.

³²⁵ NO SA Request to the EDPB, p. 11-12.

³²⁶ NO SA Request to the EDPB, p. 11-12.

181. The NO SA also recalls that in any event, the Meta IE's Consent Proposal does not eliminate the urgent need to adopt final measures³²⁹.

330.

³³¹. Therefore, in

the NO SA's view, final measures constitute '*the only way*' to stop the harm to data subjects' fundamental rights³³².

4.2.1.2 Summary of the position of the controller

182. According to Meta IE, the circumstances of the case do not justify an urgent decision of the EDPB pursuant to Article 66(2) GDPR³³³. In particular, Meta IE recalls a prior decision of the EDPB stating that '*the urgency procedure under Article 66(2) GDPR is a derogation to the standard consistency and cooperation mechanisms, it must be interpreted restrictively. Therefore, the EDPB will request final measures under Article 66(2) [GDPR] only if the regular cooperation or consistency mechanisms cannot be applied in their usual manner due to the urgency of the situation*'³³⁴.
183. In this respect, Meta IE notes that the comments received by the IE SA from the CSAs show that the cooperation and consistency mechanism being led by the IE SA (which incorporates the views of numerous CSAs in addition to the views of the NO SA), is clearly functioning in accordance with Article 60 GDPR, and argues that there is no reason to derogate from that mechanism³³⁵. For this reason, in Meta IE's view, the NO SA's invocation of Article 66(1) GDPR and the NO SA Request to the EDPB are improper³³⁶.
184. According to Meta IE, the urgency procedure interferes with the regular cooperation mechanism that the IE SA has been following to implement the IE SA Decisions³³⁷. Meta IE's view is that the process of

³²⁷ Letter of NO SA to IE SA of 11 October 2023, p. 2. See also NO SA Rejection of Meta IE's and Facebook Norway's Request for Deferred Implementation of the Coercive Fine of 7 August 2023, p. 1-2, where the NO SA gives several arguments related to the fact that Meta IE has '*not implemented any measures that would warrant lifting the Order or waiving the coercive fine, as [REDACTED] the personal data of data subjects in Norway continue to be unlawfully processed for behavioural advertising purposes [...]*',

³²⁸ NO SA Request to the EDPB, p. 11.

³²⁹ NO SA Request to the EDPB, p. 11.

³³⁰ NO SA Request to the EDPB, p. 8.

³³¹ NO SA Request to the EDPB, p. 8.

³³² NO SA Request to the EDPB, p. 12.

³³³ Letter from Meta IE to IE SA of 31 May 2023, p.5; Letter from Meta IE to IE SA regarding potential urgent proceedings of 21 June 2023, p. 4.

³³⁴ Letter from Meta IE to IE SA dated 31 May 2023, p. 5, referring to EDPB Urgent Binding Decision 01/2021, paragraphs 195-196.

³³⁵ Meta IE's Submissions of 16 October 2023, p. 4.

³³⁶ Meta IE's Submissions of 16 October 2023, p. 4.

³³⁷ Meta IE's Submissions of 26 September 2023, p. 12-13.

engagement between Meta IE and the IE SA pursuant to Articles 56(6) GDPR and Article 60(10) GDPR remains ongoing, and that there are no exceptional circumstances that would allow the NO SA to bypass such process³³⁸.

185. In addition, according to Meta IE, '*the NO SA's action directly conflicts with and undermines (i) the authority of the LSA, (ii) the role of other supervisory authorities across the EU/EEA who are appropriately engaging via the LSA-led process and (iii) the GDPR's one-stop-shop mechanism*'³³⁹.
186. Meta IE also states that the existence of a disagreement between a LSA and a CSA does not, in itself, create a situation of urgency as such³⁴⁰. In this respect, it states that '*the fact that the [NO SA] appears to disagree with [REDACTED] the [IE SA] cannot justify it resorting to the use of Article 66(2) [GDPR]*'³⁴¹. Meta IE also states that there is no precedent for a SA using Article 66(2) GDPR to seek to '*overrule and dictate the process that a LSA has put in place to assess compliance with the LSA's own orders*'³⁴².
187. Regarding the nature of the infringements, Meta IE is of the view that the NO SA does not provide evidence of their alleged seriousness, and states that behavioural advertising is a common practice, widespread beyond Meta's services³⁴³.
188. Meta IE also argues that the fact that the behavioural advertising processing has been ongoing for many years does not justify any urgency but, rather, proves that there is no new element of urgency³⁴⁴. Meta IE highlights that the processing at stake in this case is the same processing as the one that has been '*the subject of detailed consideration by the [IE SA] (...) for over 4 years and by the EDPB, with the awareness of SAs throughout*'³⁴⁵. In this respect, Meta IE also recalls that in the EDPB Urgent Binding Decision 01/2021, the EDPB has established that '*the mere continuation of processing, cannot, on its own, justify an urgent need to act*'³⁴⁶.
189. Meta IE considers that the EDPB Binding Decisions did not mandate it to rely on Article 6(1)(a) GDPR for behavioural advertising processing and did not conclude either that Article 6(1)(f) GDPR was not an

³³⁸ Letter from Meta IE to IE SA of 31 May 2023, p. 5; Letter from Meta IE to IE SA regarding potential urgent proceedings of 21 June 2023, p. 4.

[REDACTED]
[REDACTED]
[REDACTED].

³³⁹ Letter from Meta IE to the IE SA [REDACTED] of 10 August 2023, p. 2.

³⁴⁰ Meta IE's Submissions of 26 September 2023, p. 1-2, 8. See also Meta IE's Submissions of 16 October 2023, p. 5.

³⁴¹ Meta IE's Submissions of 26 September 2023, p. 12.

³⁴² Meta IE's Submissions of 26 September 2023, p. 2.

³⁴³ Meta IE's Submissions of 26 September 2023, p. 9. More specifically, Meta IE highlights that the minimum age for using Facebook and Instagram is 13 and for users aged between 13 and 17 only the age and location are used to display ads.

³⁴⁴ Meta IE's Submissions of 26 September 2023, p. 8-9. Meta IE also reiterated that the '*alleged "urgency" claimed by the [NO SA] cannot be premised on the relevant processing (i.e. [Meta IE]'s use of on-platform data for behavioural advertising purposes), given this processing has been ongoing for years with the full knowledge of regulators, and the only recent development is that [Meta IE] has increased the level of data subjects' control over this processing*', see Meta IE's Submissions of 16 October 2023, p. 5.

³⁴⁵ See also Letter from Meta IE to IE SA of 31 May 2023, p. 5. Also see Letter from Meta IE to IE SA regarding potential urgent proceedings of 21 June 2023, p. 3.

³⁴⁶ Letter from Meta IE to IE SA of 31 May 2023, p. 5, referring to the EDPB Urgent Binding Decision 01/2021, paragraphs 195-196.

appropriate legal basis for the processing of personal data collected on Meta's products for the purpose of behavioural advertising³⁴⁷. Meta IE argues that it was only with the IE SA Final Position Paper that it became clear to it that its reliance on Article 6(1)(f) GDPR for such processing did not comply with the IE SA Decisions³⁴⁸.

190. Meta IE also argues that the IE SA is not refraining from enforcing the GDPR against it, given that the IE SA shared a timeline with the CSAs and issued the IE SA Provisional Position Paper and then the IE SA Final Position Paper³⁴⁹.

[REDACTED]
350.

191. Meta IE states further that any urgent binding decision would be counterproductive [REDACTED], and ultimately harm the interests of data subjects while generating administrative work for the EDPB, the IE SA, the CSAs and Meta IE³⁵¹. In this respect, it also highlights that the measures requested by the NO SA through the urgency proceedings had already been considered as objections during the previous Article 65 GDPR process, and rejected by the EDPB in the EDPB Binding Decisions³⁵².

[REDACTED]
353.

4.2.1.3 Analysis of the EDPB

192. Article 66(2) GDPR requires the SA requesting an urgent binding decision to provide reasons for requesting such opinion. This includes the need for the requesting SA to demonstrate an urgent need to act.
193. Therefore, the EDPB analyses, whether, on the basis of the views of the NO SA and of the controller, as well as on the basis of the elements in the file, the condition of urgency is met.
194. In this respect, the EDPB considered in a past decision that the nature, gravity and duration of an infringement, as well as the number of data subjects affected and the level of damage suffered by them, may play an important part when deciding whether or not there is an urgent need to act in a particular case³⁵⁴.
195. **In relation to the nature and gravity of the infringements**, the EDPB notes that its findings that Meta IE still relies inappropriately on Article 6(1)(b) GDPR to process personal data, including location data and advertisement interaction data collected on its products for the purpose of behavioural advertising³⁵⁵ and on Article 6(1)(f) GDPR to process personal data collected on its products for the

³⁴⁷ Meta IE's Submissions of 26 September 2023, p. 10.

³⁴⁸ Meta IE's Submissions of 26 September 2023, p. 10 (Meta IE refers to national courts in the EU holding, prior to the IE SA Decisions, that Art. 6 (1) (b) GDPR is an appropriate legal basis, and to the fact that previous decisions from the IE SA initially confirmed the possibility to rely on Art. 6 (1) (b) GDPR). See also Meta IE's Submissions of 16 October 2023, p. 5.

³⁴⁹ Meta IE's Submissions of 26 September 2023, p. 7 and 9.

³⁵⁰ Meta IE's Submissions of 26 September 2023, p. 11.

³⁵¹ Meta IE's Submissions of 26 September 2023, p. 3; see also Meta IE's Submissions of 25 August 2023, paragraphs 46-48.

³⁵² Meta IE's Submissions of 26 September 2023, p. 7-8.

³⁵³ Meta IE's Submissions of 26 September 2023, p. 9.

³⁵⁴ EDPB Urgent Binding Decision 01/2021, adopted on 12 July 2021, paragraph 169.

³⁵⁵ See paragraphs 98-995 and 152 above.

purpose of behavioural advertising³⁵⁶ relate to the same processing activities as those referred to in the IE SA Decisions adopted on the basis of EDPB Binding Decisions.

196. In this respect, the EDPB recalls its finding from the EDPB Binding Decisions, i.e. that the nature and gravity of the infringement of Article 6(1) GDPR are such that a risk of damage caused to data subjects is consubstantial with the finding of the infringement itself³⁵⁷. In relation to Meta IE's infringements of Article 6(1) GDPR with respect to behavioural advertisement practices, the EDPB found that they constituted a very serious situation of non-compliance with the GDPR, in relation to processing of extensive amounts of data³⁵⁸, which is essential to the controller's business model, and harming the rights and freedoms of millions of data subjects in the EEA³⁵⁹.
197. The EDPB also already highlighted in its EDPB Binding Decisions the '*complexity, massive scale and intrusiveness of the behavioural advertising practice that [Meta IE] conducts*'³⁶⁰. This view is still currently shared by the NO SA, which finds that Meta IE's users' online activities are '*constantly, intrusively and opaqueley monitored and profiled*' by Meta IE, which '*may give rise to the feeling that their private life is being continuously surveilled*'³⁶¹. This view is also still shared by the NL SA, which expressed great concerns with respect to the processing activities at stake in light of '*the large amount of personal data being processed, the number of data subjects involved as well as the nature of the data that is being processed – including video, audio and mouse movement*'³⁶².
198. The EDPB also clarified that at the time of the adoption of the EDPB Binding Decisions, bringing the processing into compliance with the GDPR would allow to minimise the potential harm to data subjects created by the violations of the GDPR³⁶³. In the EDPB Binding Decisions, the elements of the 'nature and gravity of the infringement'³⁶⁴ and the 'number of data subjects affected' - which were and still are significant³⁶⁵ - led the EDPB to conclude that '*it is particularly important that appropriate corrective measures be imposed [...] in order to ensure that [Meta IE] complies with this provision of the GDPR*'³⁶⁶.
199. When determining the transition period for bringing Meta IE's processing into compliance with the GDPR, the EDPB requested that the IE SA gives '*due regard to the harm caused to the data subjects by the continuation of [Meta IE]'s infringement of Article 6(1) GDPR during this period*'³⁶⁷.
200. The need for urgent action was fully acknowledged and clearly indicated in the IE SA Decisions³⁶⁸.

³⁵⁶ See paragraphs 148 and 153 above.

³⁵⁷ EDPB Binding Decision 3/2022, paragraph 446 and EDPB Binding Decision 4/2022, paragraph 415.

³⁵⁸ EDPB Binding Decision 3/2022, paragraph 444 and EDPB Binding Decision 4/2022, paragraph 413.

³⁵⁹ EDPB Binding Decision 3/2022, paragraph 282 and EDPB Binding Decision 4/2022, paragraph 284.

³⁶⁰ EDPB Binding Decision 3/2022, paragraph 96 and EDPB Binding Decision 4/2022, paragraph 99.

³⁶¹ NO SA Request to the EDPB, p. 10, referring to CJEU Bundeskartellamt Judgment, paragraph 118.

³⁶² NL SA Mutual Assistance Request, p. 2.

³⁶³ EDPB Binding Decision 3/2022, paragraph 282 and EDPB Binding Decision 4/2022, paragraph 284.

³⁶⁴ EDPB Binding Decision 3/2022, paragraph 279 and EDPB Binding Decision 4/2022, paragraph 281.

³⁶⁵ EDPB Binding Decision 3/2022, paragraph 445 and EDPB Binding Decision 4/2022, paragraph 414.

³⁶⁶ EDPB Binding Decision 3/2022, paragraph 279 and EDPB Binding Decision 4/2022, paragraph 281.

³⁶⁷ EDPB Binding Decision 3/2022, paragraph 286 and Binding Decision 4/2022, paragraph 288.

³⁶⁸ IE SA FB Decision, paragraph 8.10 ('[...] I do not agree with Facebook's submission that the [IE SA] has discretion to delay the activation of the timeline for compliance [...]. It is clear, from paragraph 286 of the Article 65 [GDPR] Decision, that the EDPB considered it necessary for Facebook to take the remedial action required to address the relevant infringements "within three months". While Facebook has correctly identified that the EDPB has not expressly identified the starting point of this compliance period, the [IE SA]'s view is that it goes without saying that the starting point has to be the adoption and notification of the [IE SA]'s final decision, given that this is the earliest time from which the applicable timeline for compliance can start to run. Any contrary suggestion would

201. In relation to the **duration of the infringement** and considering the above findings that Meta IE still relies inappropriately on Article 6(1)(b) GDPR and Article 6(1)(f) GDPR to process personal data collected on its products for the purpose of behavioural advertising³⁶⁹ despite the fact that the deadline for complying with the IE SA Decisions was 5 April 2023, the EDPB finds that data subjects are still faced with data processing activities that are unlawful³⁷⁰. In relation to Meta's argument that it is only on 18 August 2023 that the IE SA concluded that Meta IE's reliance on Article 6(1)(f) GDPR for behavioural advertising purpose was insufficient to comply with the IE SA Decisions³⁷¹, the EDPB shares the view of the NL SA expressed already on 30 May 2023 that '*the controller could not have been unaware of already established guidance from the EDPB, nor of the position of several CSAs on the matter, but chose to explore the path of Article 6(1)(f) [GDPR] regardless'*³⁷².
202. In this respect, the EDPB can only note that every additional day during which the processing activity at stake takes place without reliance on an appropriate legal basis causes supplementary harm to the data subjects and allows Meta to continue to collect significant amounts of personal data of millions of European individuals on a daily basis and to generate significant revenue from the unlawful processing of the personal data of millions of data subject in the EEA³⁷³. It also observes, in line with the position of the NO SA, that there are no measures that could be applied retroactively to repair the violation of the rights and freedoms of data subjects³⁷⁴.
203. Therefore, while in some cases the fact that an infringement has been continuing for a long time may serve to demonstrate that an urgent need to act does not arise³⁷⁵, as recalled by Meta IE³⁷⁶, the EDPB considers in this case that the situation is different. To the contrary, in this case, the fact that the processing activities are still performed without reliance on an appropriate legal basis represents an element in favour of concluding that there is an urgent need for final measures to be adopted, since despite the orders given in the IE SA Decisions and the different discussions regarding their implementations, Meta IE still processes unlawfully personal data and still does not comply with the IE SA decisions³⁷⁷. This is not dispelled by Meta IE's arguments on the fact that more transparency and an opt-out mechanism were implemented³⁷⁸, as these elements do not solve the underlying issue of the lawfulness of the processing³⁷⁹ and the related harm caused on data subjects.

be inconsistent with the need for urgent action that was clearly indicated to be required in paragraphs 286, 288 and 290 of the Article 65 Decision. It would further render meaningless the EDPB's consideration of the compliance period in terms of a fixed number of months (in this case, three)'. An analogous wording is present in paragraph 214 of the IE SA IG Decision.

³⁶⁹ See paragraphs 152 and 153 above.

³⁷⁰ EDPB Binding Decision 3/2022, paragraph 446 and EDPB Binding Decision 4/2022, paragraph 415.

³⁷¹ Meta IE's Submissions of 26 September 2023, p. 11 and Meta IE's Submissions of 16 October 2023, p.5.

³⁷² NL SA Mutual Assistance Request, p. 2.

³⁷³ In this respect, Meta IE states that '*any suspension of behavioural advertising in Norway for nearly a three month period would irreparably damage [Meta IE] as it would suffer (i) many millions of Euros in lost advertising revenue during this period*', see Meta IE's Letter to the NO SA of 14 August 2023, p.9.

³⁷⁴ NO SA Rejection of Meta IE's and Facebook Norway's Request for Deferred Implementation of the Order dated 7 August 2023, p. 1.

³⁷⁵ See, for instance, EDPB Urgent Binding Decision 01/2021, paragraphs 195-196.

³⁷⁶ Letter from Meta IE to IE SA of 31 May 2023, p. 5, referring to the EDPB Urgent Binding Decision 01/2021, paragraphs 195-196.

³⁷⁷ See sections 4.1.1.4 and 4.1.2.4 above.

³⁷⁸ Meta IE's Submissions of 26 September 2023, p. 9.

³⁷⁹ See paragraphs 152 and 153 above.

204. The EDPB recalls in this respect the NO SA's argument that the failure to firmly and expediently react to non-compliance with the IE SA Decisions deprives data subjects of the protection that they are entitled to³⁸⁰.
205. The EDPB finds, in light of the above and in line with the view of the NO SA, that **failing to put an end to the processing activities at stake and to enforce the IE SA Decisions exposes data subjects to a risk of serious and irreparable harm**³⁸¹. The NO SA, alongside other CSAs, have also expressed the view that further measures are urgently needed in this case not only to address the situation of non-compliance with the GDPR but also put an end to the harm to data subjects.
206. The SE SA expressed the need for further action after the circulation of Meta IE Compliance Reports and asked '*the [IE] SA what procedure [the SE SA] can expect going forward*'³⁸².
207. The NL SA [REDACTED]
[REDACTED], echoing its previous call to the IE SA "*to swiftly undertake adequate actions in order to cease the continuous illegality of the invasive processing of personal data of millions of users*"³⁸³. It is also important to recall the NL SA Mutual Assistance Request³⁸⁵, according to which '*appropriate and expedient action is required to protect the fundamental rights of millions of data subjects in the Netherlands as well as throughout the European Economic Area*'³⁸⁶ and that SAs should be '*acting together*' on this '*as cooperating European supervisory authorities under the lead of the [IE SA]*'³⁸⁷.
208. Similarly, already after the circulation of the IE SA Provisional Position Paper to the CSAs, the DE Hamburg SA requested the IE SA '*to swiftly reach a consolidated position that [Meta IE] has not demonstrated the legal basis and suspend the processing, which is based on Art[icle] 6 (1) [(b) GDPR] and [Article 6 (1)] (f) GDPR for behavioural advertising*'³⁸⁸.
209. In the EDPB Binding Decisions, the EDPB made clear that urgent action was already required in December 2022 and decided that, at that time, the order for compliance to be imposed on Meta IE should require Meta IE to restore compliance within a short period of time³⁸⁹. In doing so, the EDPB

³⁸⁰ NO SA Request to the EDPB, p. 6.

³⁸¹ See paragraph 175 above, and NO SA Request to the EDPB, p. 10.

³⁸² SE SA comment in IE SA IMI Informal Consultations of 4 May 2023.

³⁸³ [REDACTED].

³⁸⁴ Views of the NL SA on the Compliance Reports of 4 May 2023, in IMI informal consultation on FB case and in IMI informal consultation on IG case, paragraph 4.

³⁸⁵ The NL SA made the NO SA Mutual Assistance Request on 30 May 2023 and requested the IE SA to inform them by 30 June 2023:

(i) '*Of its conclusion as to whether [Meta IE] can or cannot invoke Article 6(1)(f) GDPR for the processing of the personal data of its users for the purposes of behavioural advertising, more specifically for a large part of the processing operations for which [Meta IE] previously relied on Article 6(1)(b) [GDPR];*' and
(ii) '*Of its conclusion as to whether [Meta IE] does or does not comply with the [IE SA]'s final decision of 31 December 2022, ordering [Meta IE] to bring these processing operations in line with Article 6 GDPR;*' and
(iii) '*Of a timeframe in which appropriate and expedient action will be taken to ensure that [Meta IE] acts in compliance with Article 6 GDPR, to protect the fundamental rights of millions of data subjects affected by this processing operation, in the Netherlands as well as throughout the European Economic Area (EEA). In this respect, the [NL SA] attaches significant weight to the connection between the controller's non-compliance with Article 6 GDPR and its failure to comply with the [IE SA]'s order. In our view, this warrants prompt intervention'*

³⁸⁶ NL SA Mutual Assistance Request, p. 1.

³⁸⁷ NL SA Mutual Assistance Request, p. 2.

³⁸⁸ Views of the DE Hamburg SA on IE SA Provisional Position Paper of 21 July 2023, p. 2.

³⁸⁹ Binding Decision 3/2022, paragraph 286 and Binding Decision 4/2022, paragraph 288.

recalled the IE SA's reasoning on the three-month deadline already provided by the IE SA its draft decision³⁹⁰ for compliance for the transparency infringements, which it considered to be necessary and proportionate in light of: (1) the potential for harms to the data subjects' rights that such a measure entails, considering that the interim period for compliance '*will involve a serious ongoing deprivation of their rights*', (2) the significant financial, technological, and human resources and (3) the clear instructions provided to Meta IE to comply with GDPR³⁹¹. The EDPB therefore instructed the IE SA to include in its final decision an order for Meta IE to bring its processing of personal data for the purpose of behavioural advertising in the context of the Facebook service into compliance with Article 6(1) GDPR **within three months**³⁹².

210. Importantly, the understanding that the timeframe to be left to Meta IE to achieve compliance with the GDPR needed to be a fixed one was also shared by the IE SA in the IE SA Decisions, where the IE SA referred to the EDPB Binding Decisions and explained that clearly '*the EDPB considered it necessary for [Meta IE] to take the remedial action required to address the relevant infringements 'within three months'*' and indicated a '*need for urgent action*', and with '*a fixed number of months*'³⁹³.
211. The EDPB previously established that urgency procedures under Article 66 GDPR are derogations from the standard consistency and cooperation mechanism and that the requirements of Article 66 GDPR must be interpreted restrictively³⁹⁴. Therefore, the EDPB considers that it may request final measures under Article 66(2) GDPR only if the regular cooperation or consistency mechanisms cannot be applied in their usual manner due to the urgency of the situation³⁹⁵. Therefore, the EDPB assesses in this section whether there is a **need to derogate from the regular cooperation and consistency mechanisms in this case**.
212. In this particular case, the IE SA already adopted the IE SA Final Decisions under the one-stop-shop procedure on the basis of the EDPB Binding Decisions, containing an order for compliance with Article 6(1) GDPR. Pursuant to Article 60(10) GDPR, the controller shall notify the measures taken for complying with a decision taken in the cooperation mechanism with the LSA, which shall inform the CSAs.
213. The EDPB Guidelines on the application of Article 60 GDPR highlight that the '*obligation [of the controller to notify to the LSA the measures taken to comply with the decision] ensures the effectiveness of the enforcement. It is also the basis of possible necessary follow-up actions to be commenced by the LSA, also in cooperation with the other CSAs*'³⁹⁶.
214. These guidelines further point out that if the LSA concludes that the measures taken are insufficient, the LSA should, as part of its legal duty to inform the CSAs, consider providing the other CSAs with its assessment of the measures adopted by the controller, in particular in order to decide whether further

³⁹⁰ IE SA draft decision relating to Facebook, paragraph 8.4, IE SA draft decision relating to Instagram, paragraph 202.

³⁹¹ Binding Decision 3/2022, paragraph 286 and Binding Decision 4/2022, paragraph 288.

³⁹² Binding Decision 3/2022, paragraph 288 and Binding Decision 4/2022, paragraph 290.

³⁹³ IE SA FB Decision, paragraph 8.10; IE SA IG Decision, paragraph 214.

³⁹⁴ EDPB Urgent Binding Decision 01/2021, adopted on 12 July 2021, paragraphs 165-167.

³⁹⁵ EDPB Urgent Binding Decision 01/2021, adopted on 12 July 2021, paragraph 167. Also see paragraph 169 above.

³⁹⁶ EDPB Guidelines 02/2022 on the application of Article 60 GDPR, adopted on 14 March 2022, paragraph 248.

actions are necessary³⁹⁷. This indicates that where the measures adopted by the controller are considered to be insufficient, there may be a need for the LSA to take further actions.

215. In the case at hand, the IE SA concluded in the IE SA Final Position Paper, also relying upon the comments shared and views expressed by the CSAs, that Meta IE failed to demonstrate compliance with the IE SA Decisions³⁹⁸. However, it also considered that it was '*'fair'* and '*'reasonable'* to provide Meta IE with an opportunity to demonstrate that it can rely on consent as a lawful basis rather than engaging in enforcement measures³⁹⁹.
216. The IE SA has also reiterated its position, as LSA, that no further urgent actions are necessary in this case, as the course of action already being taken, consisting in '*an enforcement procedure [...] in which a defined set of proposals, by which [Meta IE] proposes to achieve compliance with its obligations under Article 6 GDPR (and the terms of the [IE SA] Decisions), is the subject of ongoing assessment by the [IE SA] and the CSAs*', is adequately addressing the situation⁴⁰⁰.
217. In this respect, the EDPB acknowledges the need to evaluate the proposal being made by the controller, and that this entails the '*examination of a number of particularly complex (and novel) issues*'⁴⁰¹. The EDPB also fully acknowledges that a '*regulatory process*' is '*being conducted under the GDPR's cooperation and consistency framework*', led by the IE SA,

[REDACTED]

[REDACTED] 402.

- 218.

[REDACTED] 403.

[REDACTED] 404.

The EDPB therefore finds that the existence of the Meta IE's Consent Proposal does not undermine the need to take actions to ensure that the unlawful processing comes to an end.

219. In this context, the EDPB notes that the IE SA acknowledged in its Final Position Paper - more than four months after the deadline for compliance - that Meta IE still infringes the GDPR⁴⁰⁵. The EDPB finds that the fact that the IE SA did not take supervisory measures to put an end to Meta IE's inappropriate reliance on 6(1)(b) and 6(1)(f) GDPR and to enforce the IE SA Decisions, despite the risk of serious and

³⁹⁷ EDPB Guidelines 02/2022 on the application of Article 60 GDPR, adopted on 14 March 2022, paragraph 249.

³⁹⁸ IE SA Final Position Paper, paragraph 9.2.

³⁹⁹ IE SA Final Position Paper, paragraph 9.2.

⁴⁰⁰ Letter of IE SA to NO SA of 13 October 2023, p. 4.

⁴⁰¹ Letter of IE SA to NO SA of 13 October 2023, p. 4-5.

⁴⁰² Letter of IE SA to NO SA of 13 October 2023, p. 6.

⁴⁰³ Letter of IE SA to NO SA of 13 October 2023, p. 4-5.

⁴⁰⁴ IE SA's Response to Meta IE of 11 August 2023 p. 2. The [REDACTED]

⁴⁰⁵ IE SA Final Position Paper, paragraph 8.1.

irreparable harm caused to data subjects⁴⁰⁶, shows that the regular cooperation and consistency mechanism is not providing satisfactory results, and that there is a need to request the IE SA to urgently order final measures due to the urgency of the situation. In this respect, the EDPB notes that while now six months after the deadline for compliance have passed, there is still no clear indication that compliance will be reached soon nor is there a clear indication that the IE SA - as LSA - intends to adopt corrective measures in order to end the ongoing infringements⁴⁰⁷.

220. In conclusion, the EDPB finds, in light of the circumstances described above, **that the regular cooperation or consistency mechanisms cannot be applied in their usual manner, and that due to the risk of serious and irreparable harm without urgent final measures**, there is a need to derogate from the regular cooperation and consistency mechanisms to order final measures due to the urgency of the situation.
221. Lastly, the EDPB considers it relevant to recall the SAs' duty to monitor the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU⁴⁰⁸. In particular, the EDPB has stated that when a violation of the GDPR has been established, competent supervisory authorities are required to react appropriately to remedy this infringement⁴⁰⁹. The powers afforded to SAs by Article 58 GDPR are aimed to fulfilling this goal. Similarly, the Court of Justice of the European Union held that '(...) [a]lthough the supervisory authority must determine which action is appropriate and necessary (...), the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence'⁴¹⁰.

4.2.2 On the application of a legal presumption of urgency justifying the need to derogate from the cooperation and consistency mechanisms

222. In the precedent section, the EDPB found that there is a need to derogate from the regular cooperation and consistency mechanisms to order final measures due to the urgency of the situation⁴¹¹. In this section, the EDPB assesses whether such urgency and need to derogate from the regular cooperation and consistency mechanisms may also be presumed on the basis of Article 61(8) GDPR.
223. Considering the facts of the case⁴¹², the EDPB will assess whether this case falls within the description provided by Article 61(8) GDPR, which refers to the situation where an SA does not provide the information referred to in Article 61(5) GDPR within one month of receiving a mutual assistance request from another SA. Article 61(8) GDPR provides that the '*urgent need to act under Article 66(1) [GDPR] shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2) [GDPR]*'. If such a presumption applies, the urgent nature of an Article 66(2) request for an urgent binding decision can be presumed and does not need to be demonstrated⁴¹³.

⁴⁰⁶ See paragraph 205 above.

⁴⁰⁷ See paragraphs 215-216 above

⁴⁰⁸ Article 51(1) GDPR and Recital 123 GDPR.

⁴⁰⁹ EDPB Binding Decision 3/2022, paragraph 278 and EDPB Binding Decision 4/2022, paragraph 280 (referring to CJEU Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraph 111).

⁴¹⁰ Judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, ECLI:EU:C:2020:559, paragraph 112.

⁴¹¹ See EDPB analysis under 4.2.1.3

⁴¹² See Section 1 of this urgent binding decision.

⁴¹³ EDPB Urgent Binding Decision 01/2021, adopted on 12 July 2021, paragraph 170.

224. As mentioned, the NO SA Mutual Assistance Request was made on 5 May 2023 - see paragraphs 10, 13, and 15 above describing the NO SA Mutual Assistance Request and the response provided by the IE SA.

4.2.2.1 Summary of the position of the NO SA

225. The NO SA considers that Article 61(8) GDPR is applicable in this case⁴¹⁴ because the IE SA replied 'No, I cannot comply with the request' to the NO SA Mutual Assistance Request '*without providing any specific justification other than referring to another letter it sent to all of the CSAs on 31 May 2023*'⁴¹⁵. The NO SA also argues that the '*IE SA did not provide a reasoned refusal*' as per Article 61(4) GDPR, '*nor did it inform [the NO SA] of results or progress of any measures taken in order to respond to [their] request to ban the unlawful processing of personal data and to enforce compliance with Article 6(1) [GDPR]*'⁴¹⁶. According to the NO SA, the content of the letter of 31 May 2023 was a simple announcement of when the IE SA would finalise its review of the Meta IE Compliance Reports, but it '*did not provide any information on the specific enforcement plan [they] requested, nor did it announce any specific or envisaged enforcement action with respect to Meta IE, despite [their] request to that effect*'⁴¹⁷.
226. In view of the NO SA there '*were no measures taken in order to respond to the request*', and within a month from the NO SA Mutual Assistance request, '*the IE SA had complied with neither of [their] demands*'⁴¹⁸. The NO SA also indicates that their demands remain unfulfilled due to the fact that the IE SA considers it fair and reasonable not to engage in enforcement measures despite its conclusion that Meta IE is currently failing to rely on a valid lawful basis for behavioural advertising⁴¹⁹.
227. To support the view that Article 61(8) GDPR is applicable to the present case, the NO SA refers to an opinion of Advocate General Bobek stating that where a LSA fails to address a CSA mutual assistance request, the latter may adopt provisional measures in circumstances in which '*the urgent need to act is presumed and need not be proven*'⁴²⁰. The NO SA also mentions the existence of precedent decisions applying the Article 61(8) GDPR presumption, in particular a decision from the IT SA related to Meta IE where the SA similarly considered that a failure from the LSA to address their request legitimately allowed for a derogation to the cooperation mechanism and the triggering of an Article 66 GDPR urgency procedure⁴²¹.
228. The NO SA underlines that - contrary to the factual circumstances that led the EDPB to conclude that Article 61(8) was not applicable in a previous case⁴²² - '*the communications regarding the present matter between the NO SA and the IE SA were made using the procedure for MA [Mutual Assistance]*

⁴¹⁴ NO SA Request to the EDPB, p. 7-8.

⁴¹⁵ NO SA Request to the EDPB, p. 8.

⁴¹⁶ NO SA Request to the EDPB, p. 8.

⁴¹⁷ NO SA Request to the EDPB, p. 8.

⁴¹⁸ NO SA Request to the EDPB, p. 8;

⁴¹⁹ NO SA Request to the EDPB, p. 8, referring to the IE SA Final Position Paper. It may be useful to also note that the NO SA, in its Letter to the IE SA of 21 September 2023 (p.1), states they understand the IE SA has chosen not to follow the NO SA Mutual Assistance Request because in spite of preliminarily concluding that Meta IE is still not operating in compliance with Art. 6(1) GDPR they did not indicate any corresponding enforcement measures.

⁴²⁰ NO SA Request to the EDPB, p. 9, referring to Opinion of Advocate General Bobek in Case C-645/19, Facebook Ireland and Others, paragraph 119 and paragraph 135.

⁴²¹ NO SA Request to the EDPB, p. 9, referring to Italian SA's decision of 21 December 2022 [9853406], available at <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9853406#english>.

⁴²² NO SA Request to the EDPB, p.9 referring to EDPB Urgent Binding Decision 01/2021, paragraphs. 171-181.

*requests pursuant to Article 61(1) GDPR, and not the procedure for Voluntary Mutual Assistance (“VM[A]”) requests*⁴²³.

4.2.2.2 Summary of the position of the controller

229. Meta IE argues that, in this case, no ‘*presumption of urgency arises under Article 61(8) GDPR*’⁴²⁴. Meta IE indicates that in order to rely on Article 61(8) GDPR presumption of urgency, the NO SA ‘*must show that the [IE SA] failed to respond to the [NO SA’s Mutual Assistance Request]*’ but considers that the NO SA ‘*cannot show this*’⁴²⁵. Meta IE states that the NO SA’s ‘*attempt to rely on the presumption of urgency in Article 61(8) GDPR is misconceived as a matter of law and contradicts the factual record of communications*’ between the IE SA and the NO SA⁴²⁶. According to Meta IE, the IE SA ‘*adequately addressed the [NO SA Mutual Assistance Request] by providing the information the [NO SA] requested*’ and the NO SA ‘*distort[s] and mischaracterize[s] the substance and nature of the correspondence*’ with the IE SA⁴²⁷.
230. In Meta IE’s view, the NO SA Mutual Assistance Request did not ‘*request the [IE SA] to detail a “specific enforcement plan” or “specific or envisaged enforcement action” that it would “impose on [Meta IE] in the event of non-compliance*’, as this is not what is entailed by the request of the NO SA to the IE SA to share ‘*a timeline specifying how it will ensure in an expedient manner that Meta [IE] complies with Article 6(1) GDPR*’⁴²⁸. Rather, according to Meta IE, this wording referred to a request to share a timeline, which the IE SA provided ‘*on numerous occasions*’⁴²⁹ and this demonstrates that there was ‘*no inaction or failure to communicate by the [IE SA] which the [NO SA] can now rely on to invoke Article 61(8) [GDPR]*’⁴³⁰.
231. According to Meta IE, ‘*the [IE SA]’s decision not to immediately implement the [NO SA]’s own preferred enforcement measures did not amount to a failure to adequately respond to the [NO SA Mutual Assistance Request]. Nothing in Article 61(1) GDPR requires such blind obedience by an LSA to whatever actions a CSA might request it to take. [...] The [IE SA] adequately addressed the [NO SA Mutual Assistance Request] by providing the information the [NO SA] requested*’⁴³¹. It also states that ‘*Article 61(5) GDPR [...] does not require an LSA to commit in advance to impose any specific corrective measures within any specific timeframe*’⁴³². Meta IE further elaborates that while ‘*Article 61 GDPR cannot be used by a single SA to demand that an LSA adopt corrective measures with respect to processing that is subject to an ongoing LSA-led compliance proceeding*’, the IE SA later provided reasons ‘*for declining to issue an immediate ban on processing*’⁴³³. In this regard, Meta IE is of the opinion that corrective measures cannot be requested ‘*with respect to processing that is subject to an ongoing LSA-led compliance proceeding*’ as this could ‘*undermine the one-stop shop mechanism and*

⁴²³ NO SA Request to the EDPB, p.9-10.

⁴²⁴ Meta IE’s Submissions of 25 August 2023, p. 18-21; Meta IE’s Submissions of 16 October 2023, p. 5-8; Annexure 1 to Meta IE’s 16 October 2023 Letter, p.17; Annexure 12 to Meta IE’s 16 October 2023 Letter, p.49-53.

⁴²⁵ Meta IE’s Submissions of 25 August 2023, p. 19; Meta IE’s Submissions of 16 October 2023, p. 5.

⁴²⁶ Meta IE’s Submissions of 26 September 2023, p. 5.

⁴²⁷ Meta IE’s Submissions of 16 October 2023, p. 5.

⁴²⁸ Meta IE’s Submissions of 26 September 2023, p. 5, referring to the NO SA Mutual Assistance Request.

⁴²⁹ Meta IE’s Submissions of 25 August 2023, p. 19.

⁴³⁰ Meta IE’s Submissions of 26 September 2023, p. 7.

⁴³¹ Meta IE’s Submissions of 26 September 2023, p. 2; Meta IE’s Submissions of 16 October 2023, p. 5.

⁴³² Meta IE’s Submissions of 16 October 2023, p. 5.

⁴³³ Meta IE’s Submissions of 16 October 2023, p. 6, referring to (i) Meta IE’s Merit Complaint submitted to the Oslo District Court annexed to Meta IE’s Submissions of 16 October 2023, and to (ii) the IE SA Final Position Paper.

*the LSA's duty to consider all CSAs views in connection with that mechanism'*⁴³⁴. In addition, Meta IE argues that the request ban on processing had already been '*considered and rejected by the EDPB in a prior Article 65 GDPR binding decision'*⁴³⁵.

232. In Meta IE's view, the IE SA addressed the NO SA's Mutual Assistance Request via the IE SA Update to CSAs of 31 May 2023 as it contained '*relevant information*' and allowed to inform the NO SA of '*the progress of the measures taken in order to*' address the request⁴³⁶. Considering that the IE SA did address the request on 31 May 2023, it therefore did not refuse to do so when it provided its negative response on IMI on 2 June 2023 because this response was accompanied with a reference to the IE SA Update to CSAs of 31 May 2023⁴³⁷. Meta IE further details that the IE SA had explained that the negative response on IMI was the result of a '*mistake*' and that the NO SA's message to the IE SA shows that the NO SA '*did not believe [...] that the [IE SA] had failed to respond*' to the request⁴³⁸. In support of this, Meta IE mentions a message from the NO SA to the IE SA stating: '*Thank you for your message of 2 June 2023. We understand that you will revert towards the end of June*' and '*we will await your response towards the end of June*'⁴³⁹.
233. Meta IE considers that the NO SA did not object to the IE SA Provisional Position Paper and did not mention any alleged failure by the IE SA to respond to the NO SA Mutual Assistance Request, '*despite invoking Article 61(8) GDPR in the [NO SA] Order to attempt to argue that urgency may be presumed due to an alleged failure to respond by the [IE SA]*'⁴⁴⁰. Furthermore, Meta IE argues that the NO SA '*did not raise any complaints about the [IE SA]'s proposed timetable prior to issuing the Order, even though that is what it would have been expected to do first if it had genuine concerns about urgency*'⁴⁴¹.
234. Concerning the NO SA's reference to the opinion of Advocate General Bobek in Case C-645/19, Meta IE indicates that '*considering the lengthy procedural history, which includes the [IE SA] imposing the NOYB Decisions and properly conducting an ongoing compliance procedure, the NO SA cannot reasonably argue that the [IE SA] has failed to act. The [IE SA] is acting, and also fully cooperating with, the other SAs*'⁴⁴².

4.2.2.3 Analysis of the EDPB

235. The cooperation mechanism in the GDPR provides for different tools for the SAs to exchange among themselves and perform their tasks. One of such tools is mutual assistance pursuant to Article 61 GDPR. Under this provision, SAs '*shall provide each other with relevant information and mutual assistance in order to implement and apply [the GDPR] in a consistent manner, and shall put in place*

⁴³⁴ Meta IE's Merits Complaint submitted to the Oslo District Court annexed to Meta IE's Submissions of 16 October 2023, p. 52.

⁴³⁵ Meta IE's Merits Complaint submitted to the Oslo District Court annexed to Meta IE's Submissions of 16 October 2023, p. 52, referring to (i) EDPB Binding Decision 3/2022, paragraph 285 and to (ii) EDPB Binding Decision 4/2022, paragraph 287.

⁴³⁶ Meta IE's Submissions of 16 October 2023, p. 5, referring to the IE SA Update to CSAs of 31 May 2023.

⁴³⁷ Meta IE's Submissions of 16 October 2023, p. 6.

⁴³⁸ Meta IE's Submissions of 16 October 2023, p. 6.

⁴³⁹ Meta IE's Submissions of 16 October 2023, p. 6, referring to the message sent by the NO SA to the IE SA via the IMI flow relating to the NO SA Mutual Assistance Request on 9 June 2023.

⁴⁴⁰ Meta IE's Submissions of 25 August 2023, p.9, referring to an email dated 14 July 2023 from the NO SA to the IE SA informing of the Provisional Measures being taken.

⁴⁴¹ Meta IE's Submissions of 26 September 2023, under footnote 41 p. 12.

⁴⁴² Meta IE's Complaint to the NO SA regarding the NO SA Order, 1 August 2023, p. 17; Meta IE's Submissions of 25 August 2023, p.21.

measures for effective cooperation with one another’⁴⁴³. The same provision also explains that mutual assistance ‘shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations’⁴⁴⁴.

236. The EDPB recalls that Article 61 GDPR on mutual assistance belongs to Section 1 of Chapter VII of the GDPR related to cooperation. In this regard, the EDPB considers Article 61 GDPR to be one of the mechanisms for supervisory authorities to ensure proper and efficient cooperation. Consequently, the concept of mutual assistance rooted in the GDPR entails ‘*sincere and effective cooperation*’⁴⁴⁵ and requires concrete actions from a supervisory authority receiving a mutual assistance request (hereinafter, ‘**Requested SA**’). More specifically, the obligations of a Requested SA can be listed in a logical sequence as follows:

- Article 61(2) GDPR: ‘*each SA shall take all appropriate measures required to reply to a request of another SA*’;
- Article 61(2) GDPR: the Requested SA shall reply within a specific timeframe (‘*without undue delay and no later than one month after receiving the request*’);
- Article 61(4) GDPR: the Requested SA must ‘*comply with the request*’ in all cases except for the situations mentioned in Article 61(4) (a) and (b);
- Article 61(5) GDPR, first sentence: ‘*the requested SA shall inform the requesting SA of the result or, as the case may be, of the progress of the measures taken in order to respond to the request*’;
- Article 61(5) GDPR, second sentence: ‘*the requested SA shall provide reasons for any refusal to comply with a request pursuant to paragraph 4*’;
- Article 61(6) GDPR: the Requested SA shall, as a rule, supply the information by electronic means, using a standardised format.

237. Article 61(9) GDPR provides the possibility for the European Commission (hereinafter the ‘**EC**’) to specify, by means of implementing acts, the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between SAs. On 16 May 2018, the EC adopted an implementing act relating to the use of the EC Internal Market Information system for GDPR consistency and cooperation procedures, including for Article 61 GDPR mutual assistance requests (IMI) (hereinafter, the ‘**IMI Implementing Act**’)⁴⁴⁶.
238. The IMI procedure dedicated to Article 61 GDPR mutual assistance requests is a one-to-one workflow. This entails that the request can only be addressed to, and received by, the Requested SA. Similarly, the reply will only be addressed to, and received by, the SA that made the mutual assistance request (hereinafter, the ‘**Requesting SA**’). Pursuant to Article 3(3) of the IMI Implementing Act, this dedicated workflow is to be used for the different exchanges between authorities in the framework of an Article

⁴⁴³ Article 61(1) GDPR.

⁴⁴⁴ Article 61(1) GDPR.

⁴⁴⁵ On how a ‘*lead supervisory authority cannot, in the exercise of its competences, [...] eschew essential dialogue with and sincere and effective cooperation with the other supervisory authorities concerned*’, see Judgment of the Court of Justice (Grand Chamber) of 15 June 2021, in case Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit, C-645/19, ECLI:EU:C:2021:483, paragraph 63.

⁴⁴⁶ EC Implementing Decision (EU) 2018/743 of 16 May 2018 on a pilot project to implement the administrative cooperation provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council by means of the Internal Market Information System C/2018/2814, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_2018.123.01.0115.01.ENG&toc=OJ%3AL%3A2018%3A123%3ATOC.

61 GDPR mutual assistance request. This includes, in particular, '*requesting mutual assistance from another supervisory authority in the form of information and/or supervisory measures*', '*responding to a mutual assistance request including acceptance or in exceptional cases refusals to comply with the request*', and '*communication of the progress and the result of measures taken in order to respond to the request*'⁴⁴⁷. The use of this dedicated IMI workflow also allows for the automatic monitoring of the one-month deadline to reply to a request pursuant to Article 61(2) GDPR.

239. Being a one-to-one workflow in the IMI, an Article 61 GDPR mutual assistance procedure is a type of bilateral communication to be distinguished from other bilateral or multilateral communication channels that are made available in IMI for other types of GDPR cooperation mechanisms. While a mutual assistance request can be connected to developments occurring within multilateral communication channels, the initiation of a mutual assistance request by a supervisory authority opens a dedicated workflow for exchanges between the Requesting and Requested SAs only.
240. Pursuant to Article 61 GDPR, a Requested SA is under a legal obligation to address a mutual assistance request. The only possibility for a Requested SA to refuse to address a request is where it provides reasons for refusing to comply, in line with the two limited exceptions of Article 61(4) GDPR⁴⁴⁸ and as provided in the last sentence of Article 61(5) GDPR⁴⁴⁹. While the possibility to provide information on the results or progress of the measures taken within the one-month timeframe gives some discretion to the Requested SA, the duty to cooperate also implies that the Requested SA must always take certain concrete steps to address the given request, or duly justify why it does not do so. In an exceptional situation where a Requested SA does not provide appropriate information on the measures taken, the progress made, or on the duly reasoned grounds why it cannot satisfy the request, within one month of receiving the request, the Requesting SA may consider that the conditions of Article 61(8) GDPR are met.
241. In light of the above developments, the EDPB considers that the obligation for the Requested SA to address a mutual assistance request implies the need to fulfil **procedural** and **substantive criteria**.
242. The need to fulfil the procedural criteria mainly derives from Article 61, paragraphs 6 and 9 GDPR, together with Article 3(3) of the IMI Implementing Act. The procedural criteria relate to the procedural formalities that need to be respected to address a mutual assistance request.
243. For what concerns, on the other hand, the obligation to fulfil substantive criteria, the EDPB considers that this arises from the provisions mentioned above, namely (i) the wording of Article 61(4) GDPR and Article 61 (5) GDPR, providing for a possibility to refuse to comply with mutual assistance requests only based on the limited grounds listed in the GDPR, and providing reasons for any refusal, and (ii) the qualification of mutual assistance as a tool for cooperation. This imposes the need to examine the content of the reply and the actions taken by a Requested SA to evaluate whether or not a given request has been addressed.
244. The list provided by Article 61(1) GDPR is not exhaustive ('in particular'). As such, it does not list or exclude specifically the imposition of corrective measures. However, the EDPB considers that this does

⁴⁴⁷ EC Implementing Decision (EU) 2018/743 of 16 May 2018, Article 3(3).

⁴⁴⁸ Art. 61(4) GDPR states '*The requested supervisory authority shall not refuse to comply with the request unless: (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or (b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.*'

⁴⁴⁹ 'The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4'.

not, in any event, remove the duty of the Requested SA, pursuant to Article 61 (4) and 61 (5) GDPR and the general duty of cooperation, to provide reasons for any refusal to comply with a request.

245. Moving on to the case at hand, the EDPB notes that on 5 May 2023 a formal Article 61 GDPR mutual assistance request was initiated by the NO SA via the creation of a dedicated IMI workflow. The NO SA Mutual Assistance Request contained two different requests:

- (i) '*that the IE SA issues a temporary ban on Meta IE's processing of personal data for behavioural advertising purposes on Facebook and Instagram based on Article 6(1)(f) GDPR, in accordance with Article 58(2)(f) GDPR*'⁴⁵⁰;
- (ii) '*that the IE SA shares a timeline specifying how it will ensure in an expedient manner that [Meta IE] complies with Article 6(1) GDPR*'.

246. In the NO SA Mutual Assistance Request, the NO SA also specified that they would '*be grateful if the IE SA, by 5 June 2023, would share the timeline and confirm that a temporary ban will be issued*' and that '*If the IE SA is not in a position to comply with our request regarding [Meta IE], we may need to consider our options in relation to the adoption of provisional measures in Norway pursuant to Article 66 of the GDPR. We hope that this will not be necessary and look forward to cooperating further with the IE SA within the framework of the cooperation mechanisms set out in Chapter VII of the GDPR*'.

247. The NO SA Mutual Assistance Request was also uploaded by the NO SA as a comment on the Meta IE Compliance Reports, shared with the LSA and all CSAs within the IE SA IMI Informal Consultations. Other CSAs shared their feedback on the Compliance Reports in the same period, as described above in paragraph 10, and some of them also addressed concerns on actions taken by the IE SA⁴⁵¹. In this context, on 30 May 2023, the NL SA also made a mutual assistance request, as described above in paragraph 12. Analysing, first of all, **whether the procedural criteria were met** by the IE SA's response to the NO SA Mutual Assistance Request, the EDPB notes that it is on 2 June 2023 that the first

⁴⁵⁰ The wording of the NO SA Mutual Assistance Request then goes on as follows: '*The ban should last until the lead and concerned supervisory authorities are satisfied that [Meta IE] has provided adequate and sufficient commitments to ensure compliance with Articles 6(1) and 21 GDPR, in line with Article 31 GDPR. This will give us the opportunity to further engage with Meta and make sure that it commits to fully respect its obligations under the GDPR, while preventing any further risks for data subjects stemming from [Meta IE]'s non-compliant behavioural advertising practices. Please note that in our view, behavioural advertising includes any activities where advertising is targeted on the basis of a data subject's behaviour or movements, including advertising based on perceived location*'.

⁴⁵¹ Several CSAs expressed concerns about:

(i) The IE SA not sharing its own legal assessment (e.g. FR SA on 25 April 2023; DE Hamburg SA on 4 May 2023). In response, the IE SA invited the CSAs to '*carry out their own assessments of the compliance material*' and outlined that '*the finding of infringement of Article 6(1) [GDPR] and the requirement for a corresponding order to be imposed, were determined by the EDPB*' which '*overturned the views originally expressed by the IE SA in its draft decision*' (IE SA request for CSAs views circulated via the IMI on 26 April 2023);

(ii) The measures suggested by the controller to comply with the IE SA decisions - in particular the reliance on Article 6(1)(b) GDPR and Article 6 (1)(f) GDPR for behavioural advertising - which raised concerns and criticisms for which several CSAs requested immediate actions from the IE SA (e.g. views of DE Hamburg SA on 4 May 2023; views of NL SA on 4 May 2023; comment of the SE SA on 4 May 2023).

Similarly, the NO SA had previously contacted the IE SA via email on 5 April to express their '*strong doubts*' about Meta using Article 6(1)(f) in the context of behavioural advertising, as well as their fear of a '*real risk to data subject's rights*', and asking the IE SA for their assessment and intentions for regulatory action. On 4 May 2023, the IE SA had indicated via the IE SA IMI Informal Consultations that they would '*not be preparing any further decision in this matter*' and that they would rely on their assessment of compliance, carried out jointly together with all CSAs, IE SA Information on Procedure (response to SE SA), dated 4 May 2023.

procedural development from the IE SA occurred within the Art. 61 IMI workflow initiated by the NO SA. This is when the IE SA specified they '*cannot comply with the request*' (by way of checking a pre-filled text box on IMI), and indicated in a comment they had further detailed their response under previous communications located in the IMI Informal Consultations⁴⁵². The IE SA made reference to the IE SA Update to CSAs of 31 May 2023 (see above paragraph 13). Therefore, the EDPB considers that the IE SA addressed the NO SA Mutual Assistance Request from a procedural standpoint.

248. The EDPB also analyses the **substance of the reply provided by the IE SA** to assess whether the NO SA Mutual Assistance Request was addressed within the one-month deadline set by the legislator. It is in particular relevant to assess whether the IE SA, refusing to comply with the NO SA Mutual Assistance Request, provided the reasons for such refusal in accordance with Article 61(5) GDPR. While specifying they '*cannot comply with the request*', the IE SA indicated in a comment they had further detailed their response under previous communications located in the IE SA IMI Informal Consultations⁴⁵³. The IE SA made reference to the IE SA Update to CSAs of 31 May 2023 (see above paragraph 13)⁴⁵⁴.
249. According to the IE SA, the IE SA Update to CSAs of 31 May 2023 which its reply of 2 June 2023 referred to was '*directed to the subject matter of the NO SA [Mutual Assistance Request]*' and was '*clearly engaging with the substance of the NO SA [Mutual Assistance Request] [...] directly, and in a fulsome manner*'⁴⁵⁵. Consequently, the IE SA considers it did not refuse to engage with the NO SA's request for mutual assistance by means of its communication of 2 June 2023⁴⁵⁶.
250. The content of the IE SA Update to CSAs of 31 May 2023 relates to the information about the continuation of the assessment of the Meta IE Compliance Reports pursuant to Article 60(10) GDPR⁴⁵⁷. In fact, it was a mere confirmation of the approach already suggested to all CSAs prior to the NO SA Mutual Assistance Request⁴⁵⁸.

⁴⁵² NO SA mutual assistance request IMI dedicated flow.⁴⁵³ More specifically the message from the IE SA stated: 'Dear Colleagues, Please see detailed response uploaded by the [IE SA] under [the IMI Informal Consultations] for further information. Best regards, IE SA'.

⁴⁵⁴ More specifically the message from the IE SA stated: 'Dear Colleagues, Please see detailed response uploaded by the [IE SA] under [the IMI Informal Consultations] for further information. Best regards, IE SA'. Such response was the IE SA Update to CSAs of 31 May 2023 (see paragraph 13 above). The LSA referred to two different communications issued to all CSAs via the IMI Informal Consultations.

⁴⁵⁵ The IE SA indicated that they had '*received all of the assessments from CSAs*' and '*forwarded them to [Meta IE] for it to consider the views expressed and to detail any changes that it proposes to implement on foot of the CSA assessments*'. Furthermore, the IE SA stated that it will '*complete its own assessment of [Meta IE]'s compliance reports*' '*once the IE SA receives [Meta IE]'s response*'. The IE SA also stated '*it will be in a position to complete its own assessment of [Meta IE]'s [Compliance Reports] and to share its assessment with the Norwegian and Dutch supervisory authorities (both of which have lodged Article 61 requests for mutual assistance) and with all other CSAs by the end of June 2023*'.

⁴⁵⁶ Views of IE SA on NO SA Order, p.2.

⁴⁵⁷ Views of IE SA on NO SA Order, p.2, referring to IE SA's Response to the NO SA Mutual Assistance Request.

⁴⁵⁸ The LSA indicated that they had '*received all of the assessments from CSAs*' and '*forwarded them to [Meta IE] for it to consider the views expressed and to detail any changes that it proposes to implement on foot of the CSA assessments*'. Furthermore, the LSA stated that it will '*complete its own assessment of Meta [IE]'s [C]ompliance [R]eports*' '*once the IE SA receives Meta IE's response*'. The LSA also stated '*it will be in a position to complete its own assessment of Meta's compliance reports and to share its assessment with the Norwegian and Dutch supervisory authorities (both of which have lodged Article 61 requests for mutual assistance) and with all other CSAs by the end of June 2023*'.

⁴⁵⁹ IE SA Information on Procedure (response to SE SA), dated 4 May 2023 (prior to the NO SA Mutual Assistance Request). In this communication, the LSA indicated to all CSAs - via the IMI Informal Consultations - that the '*IE SA will not be preparing any further decision in this matter*' and that they would rely on their assessment of compliance, carried out jointly together with all CSAs.

251. The EDPB notes that the IE SA Update to CSAs of 31 May 2023 makes reference to the NO SA Mutual Assistance Request, by saying: ‘The IE SA anticipates that it will be in a position to complete its own assessment of Meta IE Compliance Reports and to share its assessment with the [NO SA] and [NL SA] (both of which have lodged Article 61 requests for mutual assistance) and with all other CSAs by the end of June 2023’.
252. However, the EDPB considers that:
- the second request in the NO SA Mutual Assistance Request was a request for ‘*a timeline specifying how [the IE SA] will ensure in an expedient manner that [Meta IE] complies with Article 6(1) GDPR*’. The IE SA Update to CSAs of 31 May 2023 does provide a timeline of the next steps in the process envisaged by the IE SA for the assessment of the Meta IE Compliance Reports (with the last step being the completion of the IE SA’s own assessment and its sharing with the CSAs by the end of June 2023). However, there are no details as to how the IE SA considered that the completion of the assessment of the Compliance Reports would ‘*ensure in an expedient manner that [Meta IE] complies with Article 6(1) GDPR*’. While there is an implicit (and, in any event, only partial) connection, further motivation in this regard would have been necessary.
 - the first request in the NO SA Mutual Assistance Request was a request for the imposition of a “temporary ban on Meta’s processing of personal data for behavioural advertising purposes on Facebook and Instagram based on Article 6(1)(f) GDPR, in accordance with Article 58(2)(f) GDPR”. The IE SA Update to CSAs of 31 May 2023 does not include any reasoning as to the IE SA’s acknowledgement or consideration of this request.
253. The EDPB notes that while the IE SA explained after the expiry of the one-month deadline that the negative answer to the NO SA Mutual Assistance Request was the result of a mistake (a text box ‘incorrectly (and inadvertently) checked’)⁴⁵⁹, the IE SA does not state it tried to amend its answer - for instance to provide the reasons for any refusal to comply with the request - or sought assistance to do so within the one-month deadline.
254. The EDPB also takes note of the IE SA’s view shared on 27 September 2023 that the part of the NO SA Mutual Assistance Request pertaining to a ban was not ‘*validly made by reference to the provisions of Article 61 GDPR*’ and that it was not ‘*open to the [NO SA] to demand, by way of mutual assistance request, that the [IE SA] impose a temporary ban on the Processing Operations*’ at stake⁴⁶⁰.
255. However, Article 61(4), letter (b) GDPR envisages the possibility for the Requested SA to refuse to comply with a mutual assistance request in a situation where it considers that compliance with it would infringe the GDPR or EU or Member State law to which the Requested SA is subject. Nevertheless, in this circumstance, as already underlined under paragraph 240, the Requested SA that wishes to invoke this ground for refusal needs to motivate its response pursuant to Article 61(5) GDPR. The IE SA Update to CSAs of 31 May 2023 or the message in the MA Request workflow of 2 June 2023 do not provide any justification for not addressing the request under the limited exceptions of Article 61(4) GDPR. In addition, the views shared on 27 September 2023 were way beyond the expiration of the one month

⁴⁵⁹ Communication of IE SA to all CSAs dated 20 July 2023, p. 2.

⁴⁶⁰ Letter from the IE SA to the NO SA dated 27 September 2023, p. 3. In this regard the IE SA further argued that the EDPB Binding Decisions ‘*explicitly declined to impose a temporary ban*’ (p. 3) and that ‘*Putting in place an immediate ban on processing which is isolated and divorced from any underlying legal procedure would inevitably expose the [IE SA] to significant legal risk and lead to litigation*’ (p. 4).

deadline. Therefore, the EDPB considers that, within one month of receiving the request, the LSA did not provide the reasons for refusal to comply with the request pursuant to Article 61(5) GDPR.

256. In light of the above, the EDPB considers that the IE SA failed to provide a substantive reply the NO SA Mutual Assistance Request.
257. Considering the fact that Article 61(8) GDPR provides explicitly that the presumption of urgency applies in case the [Requested SA] does not provide the information in [Article 61(5)] within the one month of receiving the request, **the EDPB therefore considers that the presumption set by Article 61(8) GDPR is applicable in this specific case. Consequently, the EDPB finds that urgency may be presumed on the basis of Article 61(8) GDPR, which further corroborates the need to derogate from the regular cooperation and consistency mechanisms** ⁴⁶¹.

4.2.3 Conclusion as to the existence of urgency

258. The EDPB considers that the elements analysed above justify the urgency for the EDPB to request the IE SA to order final measures under Article 66(2) GDPR. The EDPB considers that the urgent need to order final measures is clear in light of the risks that the infringements represent for the rights and freedoms of the data subjects without the adoption of final measures⁴⁶². Furthermore, the EDPB considers that such urgency may be presumed pursuant to Article 61(8) GDPR⁴⁶³. **The EDPB therefore considers that there is urgency for the IE SA to order final measures in this case.**

5 ON THE APPROPRIATE FINAL MEASURES

259. On the basis of the analysis above (see sections 4.1 and 4.2), the conditions relating to the existence of infringements and to an urgent need to act in this case are met. The EDPB therefore proceeds with the analysis of which final measures, if any, it should order in this specific case. A request from a SA under Article 66(2) GDPR is aimed to address a situation where such SA, after adopting provisional measures under Article 66(1) GDPR, ‘considers that final measures need urgently be adopted’.

5.1 Content of the final measures

5.1.1 Summary of the position of the NO SA

260. In the NO SA Request to the EDPB, the NO SA requests that '*final measures, in line with the provisional measures [the NO SA] imposed in Norway, be imminently adopted*'⁴⁶⁴. In the NO SA Order, the NO SA prohibited for three months Meta IE and Facebook Norway from processing personal data of data subjects residing in Norway for behavioural advertising on the basis of Article 6(1)(b) GDPR or Article 6(1)(f) GDPR from 4 August 2023 to 3 November 2023⁴⁶⁵. The NO SA provides that the NO SA Order will be lifted before that date if remedial measures are implemented so that adequate and sufficient commitments to ensure compliance with Article 6(1) GDPR and Article 21 GDPR can be provided⁴⁶⁶. In case the order is not complied with, the NO SA announces, in the NO SA Order itself, that it may decide to impose a coercive fine of up to NOK 1 000 000 per day of non-compliance on Meta IE and/or

⁴⁶¹ Also see the EDPB Urgent Binding Decision 01/2021, paragraph 181.

⁴⁶² As demonstrated in section 4.2.2.3 above.

⁴⁶³ As demonstrated in section 4.2.1.3 above.

⁴⁶⁴ NO SA Request to the EDPB, p. 12.

⁴⁶⁵ NO SA Order, p. 3.

⁴⁶⁶ NO SA Order, p. 3.

Facebook Norway, individually or collectively⁴⁶⁷. As Meta IE and Facebook Norway did not comply with the NO SA Order, the NO SA imposed a daily coercive fine, which started to accrue on 14 August 2023⁴⁶⁸.

261. The NO SA also points out that, with respect to the objective that the final measures should seek to achieve, '*it is necessary to ensure that “[p]ersonal data shall not be processed for Behavioural Advertising based on Article 6(1)(b) [GDPR] or [Article] 6(1)(f) GDPR in the context of the Services”*'⁴⁶⁹. The NO SA requests that any final measure should demand "*swift compliance*" without further delay⁴⁷⁰.
262. With respect to the geographical scope of the final measures requested, the NO SA asked that '*the measures should be applied EEA-wide, to avoid derogating from the harmonisation and consistency that the GDPR aims to ensure*'⁴⁷¹.
263. The NO SA considers that Meta IE has a '*readily available procedure to terminate this processing rapidly*', as it already implemented an objection mechanism in the EEA in relation to its processing for behavioural advertising in reliance of Article 6(1)(f) GDPR. In other words, the NO SA argues that suspending this processing activity could be achieved through the use of a process similar to the one used by Meta IE in the context of the objection mechanism, and that nothing - from a technical perspective - prevents Meta IE from suspending the behavioural advertising processing in the EEA⁴⁷².
264. To support this request, the NO SA points out that (1) final measures should urgently be adopted because the processing of personal data violates the rights and freedoms of data subjects in all EEA states, (2) the IE SA Decisions are applicable for users in all EEA states, and (3) there is consensus at European level between the IE SA and the CSAs that the processing continues to be unlawful⁴⁷³.

5.1.2 Summary of the position of Meta IE and Facebook Norway

265. Meta IE points out that in its view '*it is not clear which final measures the [NO SA] is seeking to request from the EDPB*'⁴⁷⁴. According to Meta IE, the NO SA Order '*comprises three core elements: (i) the imposition of a temporary ban [...]; (ii) the imposition of daily administrative fines [...]; and (iii) the lifting of that ban subject to receiving adequate commitments from [Meta IE]*'⁴⁷⁵. Meta IE alleges it is not clear whether the NO SA intends to pursue each of these elements, or others, as part of its request⁴⁷⁶.
266. Meta IE considers that the NO SA Request to the EDPB constitutes partly '*an attempt to re-litigate objections that the [NO SA] has already raised in the NOYB Inquiries at the Article 65 GDPR stage and which have already been rejected by the EDPB*'⁴⁷⁷. According to Meta IE, the NO SA's actions '*appear to be motivated by (unwarranted) dissatisfaction with the [IE SA]’s handling of the enforcement of the*

⁴⁶⁷ NO SA Order, p. 4.

⁴⁶⁸ NO SA's Decision to impose a coercive fine on Meta IE and Facebook Norway of 7 August 2023, p. 3.

⁴⁶⁹ NO SA Request to the EDPB, p. 12.

⁴⁷⁰ NO SA Request to the EDPB, p. 12.

⁴⁷¹ NO SA Request to the EDPB, p. 12.

⁴⁷² NO SA Request to the EDPB, p. 12-13.

⁴⁷³ NO SA Request to the EDPB, p. 12.

⁴⁷⁴ Meta IE's Submissions of 26 September 2023, p. 13.

⁴⁷⁵ Meta IE's Submissions of 26 September 2023, p. 13.

⁴⁷⁶ Meta IE's Submissions of 26 September 2023, p. 13.

⁴⁷⁷ Meta IE's Submissions of 26 September 2023, p. 3, 13. See also Meta IE's Submissions of 16 October 2023, p. 8.

NOYB Decisions'. The controller states then that it '*cannot be sanctioned based on factors that are outside its sphere of influence*'⁴⁷⁸.

267. In addition, Meta IE provided arguments in respect of the possible content of the final measures to be ordered by the EDPB, setting out elements for each possible measure identified. Meta IE also argues that, in general, only the provisional measures adopted by the requesting SA can be adopted as final measures under the Article 66(2) GDPR procedure⁴⁷⁹. In Meta IE's view, it is unclear whether the EDPB is competent to order final measures on an EEA-wide basis, or whether it is limited to only ordering measures with respect to the country of the requesting CSA, and it is unclear whether the EDPB is competent to adopt final measures permanently⁴⁸⁰. On this matter, Meta IE also made reference to the fact that the EDPB has itself requested the EU legislator to clarify this⁴⁸¹.

268. Regarding a possible deletion order for data already unlawfully collected [REDACTED] while the NO SA has not explicitly requested such final measure, Meta IE clarified its view that such request would be unlawful and unnecessary⁴⁸². More specifically, Meta IE argues that the NO SA Order did not issue a deletion order as part of its Provisional Measures adopted under Article 66(1) GDPR⁴⁸³. Further, Meta IE highlights that the EDPB Binding Decisions rejected objections from the NO SA that aimed to impose a deletion order on Meta IE⁴⁸⁴. [REDACTED]

⁴⁸⁵ .

⁴⁸⁶ .

⁴⁸⁷. In any event, Meta IE notes that the personal data previously collected for behavioural advertising is also processed for other purposes that are not related to advertising, such as security, fraud and safety⁴⁸⁸. Meta IE considers that '*a controller cannot be compelled to delete personal data where it is validly collected and processed for different purposes pursuant to valid legal bases, even in cases where its legal basis for one distinct set of processing is subsequently held to be invalid*'⁴⁸⁹.

⁴⁷⁸ Meta IE's Submissions of 26 September 2023, p. 17.

⁴⁷⁹ Meta IE's Submissions of 26 September 2023, p. 13-14.

⁴⁸⁰ Meta IE's Submissions of 26 September 2023, p. 13, footnote 44.

⁴⁸¹ Meta IE's Submissions of 26 September 2023, p. 13, footnote 44, referring to section 6.2 of EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, at paragraphs 113-116 and 121. In this Joint Opinion, the EDPB and the EDPS provided their views on the proposed regulation made by the European Commission which, according to the EDPB and the EDPS, unduly restricts the application of the urgency procedure under Article 66(2) GDPR.

⁴⁸² Meta IE's Submissions of 26 September 2023, p. 14-15.

⁴⁸³ Meta IE's Submissions of 26 September 2023, p. 14.

⁴⁸⁴ Meta IE's Submissions of 26 September 2023, p. 14. This argument relates to the objections made by the NO SA to the draft decisions of the IE SA in the Facebook and Instagram cases, requesting an order to delete personal data processed under Art. 6(1)(b) GDPR, which the EDPB considered not to meet the threshold of Art. 4(24) GDPR (in EDPB Binding Decision 3/2022, paragraph 483 and EDPB Binding Decision 4/2022, paragraph 450).

⁴⁸⁵ Meta IE's Submissions of 26 September 2023, p. 14.

⁴⁸⁶ Meta IE's Submissions of 26 September 2023, p. 14.

⁴⁸⁷ Meta IE's Submissions of 26 September 2023, p. 14.

⁴⁸⁸ Meta IE's Submissions of 26 September 2023, p. 14-15.

⁴⁸⁹ Meta IE's Submissions of 26 September 2023, p. 15.

269. Regarding a possible suspension order or ban applicable to all EEA users, Meta IE considers that the NO SA's request for a short implementation deadline is allegedly '*flawed and not feasible*'⁴⁹⁰. According to Meta IE, building the supporting infrastructure and rolling out the objection mechanism entailed '*hundreds of thousands of hours of work*' on Meta IE's side by multi-disciplinary teams including product, machine learning and infrastructure engineers, user experience designers, operations, policy, marketing and legal to design, build and implement the systems, processes and user experience required to enable Meta IE to meet the different requirements of Article 6(1)(f) GDPR⁴⁹¹. In Meta IE's view, the NO SA's assertion that implementing a process similar to the objection mechanism could form some '*sort of instant compliance solution*' is '*flawed*'⁴⁹².

[REDACTED]
⁴⁹³. In other words, Meta IE argues that a change of legal basis for its behavioural advertising processing before [REDACTED] would simply not be feasible.

270. Meta IE also quotes the arguments put forward by the IE SA in that regard: '*Putting in place an immediate ban on processing which is isolated and divorced from any underlying legal procedure (...), would inevitably expose the [IE SA] to significant legal risk and lead to litigation. In the context of such litigation, the [IE SA] would be called on to justify its decision to depart from the course of action rooted in [IE SA Decisions] (uncontested by the EDPB and/or the CSAs), in favour of an alternative, summary procedure involving the immediate imposition of a ban on processing*'⁴⁹⁴.
271. Regarding fines specifically, Meta IE argues that the NO SA is not entitled to ask for a fine as a final measure⁴⁹⁵, since the NO SA Order did not include fines as a provisional measure under Article 66(1) GDPR. More generally, Meta IE also claims that fines are not an appropriate form of final measures under Article 66(2) GDPR⁴⁹⁶, and that the EDPB is not competent to adopt such a decision under Article 66(2) GDPR⁴⁹⁷. As the Article 66(2) GDPR procedure constitutes a derogation to the standard cooperation procedure, Meta IE, highlighting the need for a restrictive interpretation of Article 66 GDPR, is of the opinion that any final measures '*can only be those that are urgently needed to bring the infringement to an end*'⁴⁹⁸. According to Meta IE, all the final measures that do not achieve this objective must be adopted within the framework of the one-stop-shop and the consistency mechanism⁴⁹⁹. Lastly, in Meta IE's view, fines are not appropriate to ensure the immediate protection of data subjects⁵⁰⁰. Meta IE also argues that fines would be inappropriate in the circumstances of this case, where high fines have already been imposed by the IE SA in the IE SA Decisions and where Meta IE [REDACTED] engaged in good faith with the IE SA⁵⁰¹.

⁴⁹⁰ Meta IE's Submissions of 26 September 2023, p. 15.

⁴⁹¹ Meta IE's Submissions of 26 September 2023, p. 15.

⁴⁹² Meta IE's Submissions of 26 September 2023, p. 15.

⁴⁹³ Meta IE's Submissions of 25 August 2023, p. 23-24.

⁴⁹⁴ Meta IE's Merits Complaint submitted to the Oslo District Court, p. 26, referring to the Letter of the IE SA to the NO SA of 27 September 2023.

⁴⁹⁵ Meta IE's Submissions of 26 September 2023, p. 3.

⁴⁹⁶ Meta IE's Submissions of 26 September 2023, p. 16.

⁴⁹⁷ Meta IE's Submissions of 26 September 2023, p. 16.

⁴⁹⁸ Meta IE's Submissions of 26 September 2023, p. 16.

⁴⁹⁹ Meta IE's Submissions of 26 September 2023, p. 16.

⁵⁰⁰ Meta IE's Submissions of 26 September 2023, p. 16.

⁵⁰¹ Meta IE's Submissions of 26 September 2023, p. 16.

According to Meta IE, the

NO SA Request to the EDPB ‘already has, and will continue to, generate a huge amount of administrative work for the EDPB, the CSAs, the LSA and Meta [IE],’

⁵⁰². Meta IE considers that, in light of the fact that a potential urgent binding decision may extend beyond Norway, ‘any attempt to perpetuate the provisions of the [NO SA] Order by way of such a decision only serves to exacerbate this misuse of the urgency procedure and the violation of [Meta IE]’s rights’⁵⁰³.

272. Facebook Norway highlights that it is not, and has never been, a party to the inquiries leading to the adoption of the IE SA Decisions⁵⁰⁴. It also highlights that the IE SA Decisions are only addressed to Meta IE, in its capacity of sole data controller for the purpose of behavioural advertising on Facebook and Instagram. Facebook Norway points out that it is a separate and independent legal entity that does not offer Facebook or Instagram either in Norway or elsewhere, and is not the data controller for the concerned behavioural advertising processing⁵⁰⁵. Furthermore, Facebook Norway maintains that it should not have been the addressee of the NO SA Order⁵⁰⁶.
273. Meta IE and Facebook Norway have also expressed the view that the IE SA has already exercised corrective powers against Meta IE in the IE SA Decisions, and that anyways the enforcement of corrective orders is a matter for the LSA and governed by the applicable national law⁵⁰⁷.

5.1.3 Analysis of the EDPB

274. In addition to the elements enshrined in the NO SA Request to the EDPB, the EDPB takes into consideration the elements and arguments put forward by the IE SA. The IE SA considers that the NO SA Request to the EDPB seeks to obtain an urgent binding decision from the EDPB, ‘the net effect of which would be to compel the [IE SA], as LSA, to impose an EEA-wide ban’⁵⁰⁸. However, according to the IE SA, it is already leading an ongoing ‘enforcement procedure’, whereby it is, along with the CSAs, assessing ‘a defined set of proposals, by which [Meta IE] proposes to achieve compliance’ with Article 6(1) GDPR and the IE SA Decisions⁵⁰⁹. This process is happening by involving the CSAs in accordance with the GDPR’s cooperation and consistency framework⁵¹⁰. More specifically, the IE SA highlights that it ‘is currently engaged in a cooperative process to give effect to these orders in a manner that permits all CSAs to make observations on [Meta IE]’s proposed course of action’⁵¹¹.

⁵⁰² Meta IE’s Submissions of 16 October 2023, p. 9.

⁵⁰³ Meta IE’s Submissions of 25 August 2023, p. 28.

⁵⁰⁴ Facebook Norway’s Submissions of 25 August 2023, p. 13. See also Facebook Norway’s Submissions of 16 October 2023, p. 4.

⁵⁰⁵ Facebook Norway’s Submissions of 25 August 2023, p. 13; Facebook Norway’s Submissions of 16 October 2023, p. 4; see also Letter from Facebook Norway to Ministry of Local Government and Regional Development of 8 August 2023, p. 2.

⁵⁰⁶ Facebook Norway’s Submissions of 26 September 2023, p. 1. See also Facebook Norway’s Submissions of 16 October 2023, p. 4.

⁵⁰⁷ Meta IE’s and Facebook Norway’s Submissions of 19 October 2023, p. 1-2.

⁵⁰⁸ Letter from the IE SA to the NO SA of 13 October 2023, p. 3.

⁵⁰⁹ Letter from the IE SA to the NO SA of 13 October 2023, p. 4.

⁵¹⁰ Communication of IE SA to CSAs of 20 July 2023, p. 1. See also Letter from the IE SA to the NO SA of 13 October 2023, p. 4-6.

⁵¹¹ Letter from the IE SA to the NO SA of 27 September 2023, p. 3

275. According to the IE SA, no final measures ordered by the EDPB would be appropriate, as it would divert resources from the IE SA-led process under the GDPR's cooperation and consistency framework⁵¹². In addition, according to the IE SA, the NO SA's legal justifications to suggest immediate enforcement action by the LSA are '*rooted in hypothetical arguments*'⁵¹³.
276. In this regard, the EDPB acknowledges that, since the moment the IE SA shared with the CSAs the Compliance Reports on 5 April 2023, there has been an ongoing process consisting in the assessment of the compliance efforts by Meta IE represented by the switch on 3 April 2023 to Article 6(1)(f) GDPR as legal basis for most of the personal data collected on Meta's products for behavioural advertising purposes and later on, by the Meta IE's Consent Proposal, and that this process was led by the IE SA in its role as LSA in cooperation with the CSAs, which were invited to submit their views on multiple occasions.
277. However, in light of the elements described above, namely the existence of ongoing infringements of Article 6(1) GDPR - that the EDPB has already labelled as a 'very serious situation of non-compliance'⁵¹⁴, and of the duty to comply with decisions of SAs, and the existence of an urgent need to act despite the ongoing process led by the IE SA, as motivated above in Section 4.2 of this urgent binding decision, the EDPB considers that, at this point of time, there is a **need to order final measures as further enforcement measures are necessary**.
278. With respect to the **possible content of the specific final measures**, the EDPB considers that it can order final measures other than the provisional measures adopted under Article 66(1) GDPR or than those referred to in the request made pursuant to Article 66(2) GDPR. The GDPR does not indeed provide such limitations on the final measures, and the EDPB, while taking into consideration the request made pursuant to Article 66(2) GDPR as well the other elements of the file, is entrusted to ensure the correct and consistent application of GDPR when performing activities under the consistency mechanism⁵¹⁵. Therefore, the EDPB is competent under Article 66(2) GDPR to order the final measures that are appropriate on the basis of the circumstances of the case.
279. **In the case at hand, the EDPB considers it appropriate to analyse whether a ban on processing should be imposed**, bearing in mind that the NO SA Request to the EDPB asks that '*final measures, in line with the provisional measures [the NO SA] imposed in Norway, be imminently adopted*'⁵¹⁶, and that the NO SA Order included a prohibition from processing personal data of data subjects residing in Norway for behavioural advertising on the basis of Article 6(1)(b) GDPR or Article 6(1)(f) GDPR.
280. In respect of the possible imposition of a ban on processing, the IE SA considers that 'the form of order sought by the [NO SA] is not one that could lawfully be delivered by the [IE SA] in the manner now demanded'⁵¹⁷. This is, first, because the EDPB declined to instruct the IE SA to impose a temporary ban

⁵¹² Letter from the IE SA to the NO SA of 13 October 2023, p. 5.

⁵¹³ Letter from the IE SA to the NO SA of 27 September 2023, p. 4. 

⁵¹⁴ EDPB Binding Decision 3/2022, paragraph 282 and EDPB Binding Decision 4/2022, paragraph 284.

⁵¹⁵ Art. 63 GDPR, Art. 65 GDPR, Art. 70(1) GDPR, Art. 70(1)(a) GDPR, and Art. 70(1)(t) GDPR.

⁵¹⁶ NO SA Request to the EDPB, p. 12.

⁵¹⁷ Letter from the IE SA to the NO SA of 27 September 2023, p. 3.

in the EDPB Binding Decisions⁵¹⁸, and secondly because the IE SA Decisions ‘made provision for enforcement measures, namely, the orders for compliance, under which [Meta IE]’s proposals for the adoption of one or more alternative legal bases for the Processing Operations would be assessed, and ruled on, on their respective merits’⁵¹⁹. The IE SA concludes that *‘the EDPB recognised, explicitly, that a process would need to be put in place in which the Controller would identify the means by which it proposed to achieve compliance with its obligations, and, further, that, acting together in the context of the co-operation and consistency mechanism provided for at Chapter VII of the GDPR, the [IE SA] and the CSAs would in turn be required to test those proposals and assess whether or not they are sufficient to achieve compliance with the requirements of Article 6(1) [GDPR] and the [IE SA] Decisions’*⁵²⁰.

281. According to the IE SA, the imposition of a ban on processing ‘which is isolated and divorced from any underlying legal procedure would inevitably expose the [IE SA] to significant legal risk and lead to litigation’, where the IE SA ‘would be called on to justify its decision to depart from the course of action rooted in [the IE SA Decisions] (uncontested by the EDPB and/or the CSAs), in favour of an alternative, summary procedure involving the immediate imposition of a ban on processing’⁵²¹. In this regard the IE SA also argues that ‘it is inaccurate to suggest that the [IE SA] could impose an immediate ban on processing, whilst continuing to progress its assessment of [Meta IE]’s proposed consent model, in conjunction with its CSA colleagues’⁵²².
282. In this respect, the EDPB highlights that the fact that it chose not to instruct the IE SA to impose a temporary ban in the EDPB Binding Decisions, considering at that time that the imposition of an order to bring processing into compliance within a short time frame would be appropriate, does not in itself rule out the possibility than a ban would be needed today. Likewise, the fact that the IE SA Decisions, adopted on the basis of the EDPB Binding Decisions, do not provide for a ban on processing does not prevent the EDPB from ordering final measures in the form of a ban on processing in the context of this urgent procedure, taking into account the facts that occurred following the adoption of the IE SA Decisions. In this regard, the EDPB also recalls that the IE SA acknowledged in the IE SA Final Position Paper that ‘enforcement measures may [...] have been necessary at this juncture’⁵²³.
283. In the next paragraphs, the EDPB will assess the appropriateness, necessity and proportionality of a ban on processing. Article 58(2)(f) GDPR provides supervisory authorities with the power to impose a temporary or definitive limitation including a ban on processing.
284. Recital 129 GDPR provides elements to assess whether a specific measure is appropriate. More specifically, consideration should be given to ensuring that the measure chosen does not create ‘superfluous costs’ and ‘excessive inconveniences’ for the persons concerned in light of the objective pursued. When choosing the appropriate corrective measure, there is a need to assess whether the chosen measure is necessary to enforce the GDPR and achieve protection of the data subjects with regard to the processing of their personal data, which is the objective being pursued. Compliance with

⁵¹⁸ Letter from the IE SA to the NO SA of 27 September 2023, p. 3. See also Letter from the IE SA to the NO SA of 13 October 2023, p. 3-4 (where the IE SA also states the EDPB did not instruct the IE SA to adopt an automatic ban or a ban to be imposed should Meta IE fail to achieve compliance within a defined date).

⁵¹⁹ Letter from the IE SA to the NO SA of 27 September 2023, p. 3.

⁵²⁰ Letter from the IE SA to the NO SA of 13 October 2023, p. 4.

⁵²¹ Letter from the IE SA to the NO SA of 27 September 2023, p. 4.

⁵²² Letter from the IE SA to the NO SA of 27 September 2023, p. 4.

⁵²³ IE SA Final Position Paper, paragraph 9.2.

the principle of proportionality requires ensuring that the chosen measure does not create disproportionate disadvantages in relation to the aim pursued⁵²⁴.

285. As a first element, the EDPB would like to recall its reasoning in the EDPB Binding Decisions. In such decisions, as pointed out by the IE SA and by Meta IE, the EDPB analysed at that point of time whether a ban constituted an appropriate corrective measure to be imposed in the IE SA Decisions, due to the presence of some relevant and reasoned objections putting forward this request⁵²⁵. Several of the elements that the EDPB considered at the time are helpful to be considered in this urgent binding decision, too.
286. **The EDPB highlighted in the EDPB Binding Decisions** that the infringement of Article 6(1) GDPR found in the case at hand constituted a very serious situation of non-compliance with the GDPR, in relation to processing of extensive amounts of data, which is essential to the controller's business model, thus harming the rights and freedoms of millions of data subjects in the EEA; therefore, the corrective measure chosen in the circumstances of this case should aim to bring the processing into compliance with the GDPR thus minimising the potential harm to data subjects created by the violations of the GDPR⁵²⁶.
287. Therefore, according to the EDPB Binding Decisions, considering the nature and gravity of the infringement of Article 6(1)(b) GDPR, as well as the number of data subjects affected, it was particularly **important that appropriate corrective measures be imposed**, in addition to a fine, in order to ensure that Meta IE complies with this provision of the GDPR⁵²⁷.
288. It is also important to note that the EDPB considered that it is **not necessary to establish an urgent necessity for imposing a temporary ban** because nothing in the GDPR limits the application of Article 58(2)(f) GDPR to exceptional circumstances⁵²⁸.
289. While in the EDPB Binding Decisions the EDPB took note of the elements raised by the objections to justify the need for imposing a temporary ban, consisting in essence in the need to halt the processing activities that are being undertaken in violation of the GDPR until compliance is ensured in order to avoid further prejudicing data subject rights, it considered that the objective of ensuring compliance and bringing the harm to the data subjects to an end could be adequately met also by amending the order to bring processing into compliance envisaged in the IE SA draft decisions to reflect Meta IE's

⁵²⁴ EDPB Binding Decision 3/2022, paragraph 284 and EDPB Binding Decision 4/2022, paragraph 286.

⁵²⁵ More specifically, in the dispute leading to the adoption of EDPB Binding Decision 3/2022, certain objections requested the imposition of a ban or limitation on processing or an order to abstain from the processing activities in the absence of a valid legal basis (in particular, the objections of the AT, NL, DE and NO SAs). The EDPB analysed the merits of the objections of the AT and NL SAs (found to be relevant and reasoned in paragraph 266 of EDPB Binding Decision 3/2022) and did not take any position on the merits of the other objections on this matter that were found to be not relevant and reasoned, namely the objections of the DE and NO SAs (see paragraph 268 of Binding Decision 3/2022).

Concerning, instead, the dispute leading to the adoption of EDPB Binding Decision 4/2022, certain objections requested the imposition of a ban or limitation on processing or an order to abstain from the processing activities in the absence of a valid legal basis (in particular, the objections of the AT, NL, DE and NO SAs). The EDPB analysed the merits of the objections of the AT and NL SAs (found to be relevant and reasoned in paragraph 269 of EDPB Binding Decision 4/2022) and did not take any position on the merits of the other objections on this matter that were found to be not relevant and reasoned, namely the objections of the DE and NO SAs (see paragraph 271 of Binding Decision 4/2022).

⁵²⁶ EDPB Binding Decision 3/2022, paragraph 282 and EDPB Binding Decision 4/2022, paragraph 284.

⁵²⁷ EDPB Binding Decision 3/2022, paragraph 279 and EDPB Binding Decision 4/2022, paragraph 281.

⁵²⁸ EDPB Binding Decision 3/2022, paragraph 283 and EDPB Binding Decision 4/2022, paragraph 285.

infringement of Article 6(1) GDPR⁵²⁹. The EDPB noted in this regard that this measure would require Meta IE to put in place the necessary technical and operational measures to **achieve compliance within a set timeframe**⁵³⁰. Such timeframe was established to be necessarily a ‘short period of time’⁵³¹. The EDPB Binding Decisions comprised, eventually, instructions to the IE SA to include in the IE SA Decisions orders for Meta IE to bring its processing of personal data for the purpose of behavioural advertising in the context of the Facebook service into compliance with Article 6(1) GDPR within three months⁵³². In this respect, the EDPB considered this deadline for compliance to be necessary and proportionate, considering that **the interim period for compliance ‘will involve a serious ongoing deprivation of their rights’ and the significant financial, technological, and human resources available to Meta IE**⁵³³.

290. The fact that the **three-month timeframe has expired several months ago** is an important element to be considered, that marks a significant difference compared to the situation that the EDPB analysed in the EDPB Binding Decisions. Already the three-month interim period for compliance was considered by the EDPB to involve ‘*a serious ongoing deprivation*’ of data subjects’ rights: the need to ensure that this deprivation comes to an end is therefore even clearer now that three times the time initially envisaged has passed.
291. As a consequence, the reasoning of the EDPB in the EDPB Binding Decisions on whether a ban needed to be imposed in the IE SA Decisions provides **arguments in favour of considering that the imposition of a ban would be appropriate, necessary and proportionate today, rather than against this**.
292. The EDPB also takes note of the NO SA’s argument that Meta IE has a ‘*readily available procedure to terminate this processing rapidly*’, as it already implemented an objection mechanism in the EEA in relation to its processing for behavioural advertising in reliance of Article 6(1)(f) GDPR, which allows the suspension of the processing⁵³⁴.
293. The EDPB also notes Meta IE’s argument that a short implementation deadline would not be feasible⁵³⁵, considering the need for a complex process for the implementation of a ban involving several teams and many hours of work⁵³⁶. More specifically, Meta contests that it can comply ‘(i) through blanket application of the [objection mechanism] to all users across the EEA, and then “as a next step” (ii) “expanding the [objection mechanism] to include categories of data processing covered by the [NO SA Order]”, since already the NO SA acknowledges for step (ii) that this “would require redesigning the [objection mechanism]”’⁵³⁷.

⁵²⁹ EDPB Binding Decision 3/2022, paragraph 285 and EDPB Binding Decision 4/2022, paragraph 287. In reaching this conclusion, the EDPB highlighted that compliance with the principle of proportionality requires ensuring that the chosen measure does not create disproportionate disadvantages in relation to the aim pursued, and Recital 129 GDPR provides that consideration should be given to ensuring that the measure chosen does not create ‘superfluous costs’ and ‘excessive inconveniences’ for the persons concerned in light of the objective pursued. EDPB Binding Decision 3/2022, paragraph 284 and EDPB Binding Decision 4/2022, paragraph 286.

⁵³⁰ EDPB Binding Decision 3/2022, paragraph 285 and EDPB Binding Decision 4/2022, paragraph 287.

⁵³¹ EDPB Binding Decision 3/2022, paragraph 286 and EDPB Binding Decision 4/2022, paragraph 288.

⁵³² EDPB Binding Decision 3/2022, paragraph 288 and EDPB Binding Decision 4/2022, paragraph 290.

⁵³³ EDPB Binding Decision 3/2022, paragraph 286 and EDPB Binding Decision 4/2022, paragraph 288.

⁵³⁴ NO SA Request to the EDPB, p. 12-13.

⁵³⁵ Meta IE’s Submissions of 26 September 2023, p. 15.

⁵³⁶ Meta IE’s Submissions of 26 September 2023, p. 15.

⁵³⁷ Meta IE’s Submissions of 26 September 2023, p. 15 (‘Ignoring [Meta IE]’s arguments, the [NO SA] claims that [Meta IE] can comply (i) through blanket application of the [objection mechanism] to all users across the EEA, and then “as a next step” (ii) expanding the [objection mechanism] to include categories of data processing

294. According to the EDPB, the NO SA's argument on the existence of the objection mechanism is reasonable at least for what concerns the processing currently carried out on the basis of Article 6(1)(f) GDPR (i.e. the majority of the processing of personal data collected on Meta's products currently carried out for the purposes of behavioural advertising)⁵³⁸, also considering that Meta IE did not explain why for the processing based on Article 6(1)(f) GDPR a 'redesigning' of the mechanism would be necessary; also, Meta IE confirms that 'all relevant objections' are honoured leading to the 'the user [being] "opted out" of this processing'⁵³⁹.
295. Additionally, while certainly the imposition of a ban causes significant disadvantages to the controller⁵⁴⁰, the EDPB considers that such disadvantages are not at this point in time, *per se*, disproportionate compared to the harm caused to data subjects by the unlawful processing and continued non-compliance. In this regard, moreover, the EDPB notes that the controller was granted the opportunity to take remedies without facing these disadvantages. As highlighted above⁵⁴¹, several months have passed since the adoption of the IE SA Decisions and the expiry of the deadline for the orders to bring processing into compliance contained therein. At this stage, the controller has undertaken efforts to comply with the GDPR but compliance has not yet been achieved, as indicated in the IE SA Final Position Paper, and there is still no clear indication that compliance will be reached soon⁵⁴². The imposition of an order to bring processing into compliance within a short deadline did not succeed in reaching the objective it pursued, consisting in '*ensuring compliance and bringing the harm to the data subjects to an end*'⁵⁴³.

covered by the [NO SA Order]. As the [NO SA]'s argument itself acknowledges in step (ii), compliance with the [NO SA Order] (or an urgent binding EDPB decision based on the [NO SA Order]) would require redesigning the [objection mechanism]. As a reminder, building the supporting infrastructure and rolling out the [objection mechanism] entailed hundreds of thousands of hours of work by multi-disciplinary teams including product, machine learning and infrastructure engineers, user experience designers, operations, policy, marketing and legal to design, build and implement the systems, processes and user experience required to enable [Meta IE] to meet the different requirements of Article 6(1)(f) GDPR. The [NO SA]'s speculative assertion that this could form some sort of instant compliance solution is fundamentally flawed').

⁵³⁸ See Meta IE Compliance Report on IE SA FB Decision, paragraphs 3.1.3 and 5.8.2, and Meta IE Compliance Report on IE SA IG Decision, paragraphs 3.1.3 and 5.8.2. See also paragraphs 103-106 above.

⁵³⁹ Meta IE's Merits Complaint submitted to the Oslo District Court on 16 October 2023, p. 14-15 ('since the launch of the Objection Mechanism, Meta [IE] has honoured all relevant objections without qualification and without undertaking a balancing assessment to determine whether it has compelling legitimate grounds to override the user's objection. All that is checked is that the objection (i) relates to behavioural advertising processing that Meta [IE] presently undertakes under Article 6(1)(f) GDPR, and (ii) is submitted by a genuine user based in the EU/EEA (to confirm Meta [IE] is the controller and the GDPR applies). As soon as Meta [IE]'s operations team have confirmed (i) and (ii) based on the limited information that the user is asked to provide, the user is "opted-out" of this processing').

This is without prejudice to the conclusion of the IE SA in the IE SA Final Position Paper whereby the compliance with the GDPR of the objection mechanism set up by Meta IE has not been demonstrated (paragraphs 7.60-7.66).

⁵⁴⁰ In Meta IE's Letter to the NO SA of 14 August 2023, Meta IE lists challenges possibly arising from 'stopping' processing of personal data of Norwegian users for behavioural advertising purposes, involving the need to make changes to Meta IE's code and related infrastructure, inform users, provide advertisers with appropriate advance notice, waiting for users to update their apps. Meta IE also highlights the possible damage arising from a suspension of behavioural advertising in Norway, connected to lost revenue, reputational harm, and future revenue losses (p. 8-10).

⁵⁴¹ See paragraph 290 above. See also Meta Ireland's Submissions of 25 August 2023, p. 23-24; Letter from Meta Ireland to NO SA of 14 August 2023, p. 8-9.

⁵⁴² See also Meta IE's Submissions of 25 August 2023, p. 23-24; Letter from Meta IE to NO SA of 14 August 2023, p. 8-9. .

⁵⁴³ EDPB Binding Decision 3/2022, paragraph 285 and EDPB Binding Decision 4/2022, paragraph 287.

296. In light of the elements above, the EDPB considers it **appropriate, necessary and proportionate to order final measures consisting in a ban on processing**, to be adopted on the basis of Article 58(2)(f) GDPR.
297. The EDPB considers that, in this particular case, it would be proportionate that **a period of implementation be provided to enable Meta IE to implement it**.
298. The EDPB seizes the occasion to specify that also the NO SA Order was issued on 14 July 2023 but envisaged that it would only become applicable as of 4 August 2023⁵⁴⁴.
299. At the same time, the period of implementation should be a short one, in light of the urgency of the situation as described extensively in the sections above of this urgent binding decision and in particular of the urgent need to put an end to the unlawful processing being carried out to the detriment of data subjects.
300. According to the EDPB, in light of the elements in the file, the implementation of a ban in a short period of time should be technically and practically feasible for Meta IE. This is in particular the case considering that Meta IE already envisages the implementation of a consent mechanism [REDACTED]. Additionally, Meta IE has been aware of the need to bring the unlawful processing to an end since the notification of the IE SA Decisions adopted in December 2022.
301. Therefore, the EDPB considers that, in this particular case, **it is proportionate for the ban on processing to be effective one week after the notification of the final measures to the controller**.
302. Additionally, the EDPB clarifies that the ban should refer to **Meta IE's processing of personal data collected on Meta's products for behavioural advertising purposes on the basis of Article 6(1)(b) GDPR and Article 6(1)(f) GDPR**. The processing activities to which the ban refers are: (i) the processing of personal data, including location data and advertisement interaction data, collected on Meta's products for behavioural advertising purposes, having established in this respect the infringement of Article 6(1) GDPR arising from inappropriate reliance on Article 6(1)(b) GDPR; (ii) processing of personal data collected on Meta's products for behavioural advertising purposes, having ascertained in this respect the infringement of Article 6(1) GDPR arising from inappropriate reliance on Article 6(1)(f) GDPR⁵⁴⁵.
303. The EDPB considers that, in general, the **geographical scope** of the final measures ordered pursuant to Article 66(2) GDPR should be broader than the territory of the requesting SA. While it is provided by Article 66(1) GDPR that the urgent provisional measures adopted by a requesting SA only apply to the territory of that SA, the intervention of the EDPB aims to ensure a consistent application of the GDPR, in light of Articles 63 and 70 GDPR. The final measures should therefore have a broader geographical scope to ensure the protection of the rights and freedoms of all the data subjects affected; this scope can, depending on the matter, cover several Member States⁵⁴⁶. The NO SA requested that final measures, if any, 'should be applied EEA-wide, to avoid derogating from the harmonisation and consistency that the GDPR aims to ensure'⁵⁴⁷. Since in this case the unlawful processing takes place and affect the rights and freedom of data subjects in the entire EEA, the EDPB agrees that the appropriate territorial scope is for the final measures to be applicable throughout the entire EEA, and

⁵⁴⁴ NO SA Order, p. 3-4.

⁵⁴⁵ A more thorough analysis can be found above in paragraphs 97-99, 103-104, 147-148 and 152-153.

⁵⁴⁶ EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, paragraph 114.

⁵⁴⁷ NO SA Request to the EDPB, p. 12.

concurs with the NO SA on the need to avoid fragmentation in the protection afforded to data subjects. Limiting the scope of the final measures to the Norwegian territory would indeed lead to fragmentation in the protection as it would require each CSAs to adopt provisional measures on its own territory under Article 66(1) GDPR and to request an EDPB urgent binding decision under Article 66(2) GDPR leading to the need to adopt final measures limited to their own territory. Such situation could also result in a patchwork of final measures and a fragmentation in countries where the SA has not acted⁵⁴⁸.

304. The EDPB considers that the addressee of the final measures consisting of a ban on processing should be Meta IE, which shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the EEA. In line with this, and since Facebook Norway was subject to the NO SA Order alongside Meta IE and considering its submissions, Facebook Norway – which is the Norwegian establishment of Meta IE – should be informed of the outcome and receive a copy of the final measures and of the EDPB urgent binding decision.

5.1.4 Conclusion

305. In light of all the elements above, the EDPB considers it necessary to order final measures, consisting in a ban on processing pursuant to Article 58(2)(f) GDPR.
306. This ban on processing should be addressed to Meta IE, and become effective one week after the notification of the final measures to them.
307. The EDPB considers that the ban should refer to Meta IE's processing of personal data for behavioural advertising purposes on the basis of Article 6(1)(b) GDPR and Article 6(1)(f) GDPR across the entire EEA, as described above in paragraphs 303-304.

5.2 Adoption of the final measures and notification to the controller

308. The GDPR does not specify the procedural steps to be taken following the adoption of an urgent binding decision by the EDPB pursuant to Article 66(2) GDPR. It is however important to note that the two-week deadline for adoption is specified 'by derogation from [...] Article 65(2) [GDPR]' (Article 66(4) GDPR). Consequently, the EDPB considers that, in addition to Article 65(2) GDPR, the procedure set by Article 65(5) GDPR and Article 65(6) GDPR represents a point of reference.
309. The EDPB's urgent binding decision shall be addressed to the LSA and to all the CSAs and be binding on them⁵⁴⁹. The Chair of the Board shall notify, without undue delay, the urgent binding decision to the supervisory authorities concerned, and inform the European Commission thereof⁵⁵⁰.
310. Taking into consideration that the final measures will have to be applicable throughout the entire EEA (as provided in the above sections 5.1.3 and 5.1.4), the EDPB considers that the IE SA, in its role of LSA, will have to adopt a national decision imposing the measures that the EDPB has considered necessary

⁵⁴⁸ EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, paragraph 115.

⁵⁴⁹ Art. 65(2) GDPR. According to Art. 66(4) GDPR, this provision is derogated in respect of the deadline for adoption; therefore, the last sentence of Art. 65(2) GDPR fully applies.

⁵⁵⁰ See Art. 65(5) GDPR. Considering the fact that the NO SA was the SA making the request pursuant to Article 66(2), the EDPB will also inform the EFTA Surveillance Authority, in light of Article 1, second paragraph, letter m of Decision of the EEA Joint Committee No. 154/2018.

to order as final measures pursuant to Article 66(2) GDPR⁵⁵¹. This was already envisaged by the IE SA itself⁵⁵².

311. While the procedure set by Article 65(5) GDPR and Article 65(6) GDPR represents a point of reference, as mentioned above, the EDPB considers that the deadline set in Article 65(6) for the SA to adopt its national decision (one month in Article 65 proceedings) may need to be shortened, on a case by case basis, in Article 66 proceedings. The urgency of the procedure is highlighted by the shortening of the deadline for the Board to adopt its urgent binding decision or opinion under Article 66(4) GDPR. It would therefore be counterintuitive, and against the legislator's will, to imagine that the deadline for the SA to adopt its national decision should remain unchanged in Article 66 proceedings. While the EDPB acknowledges the need for time allowing the SA to draft a national decision and possibly hear the company, in this particular case it is necessary to bear in mind the date of expiry of the Provisional Measures (3 November 2023) as well as the prolonged situation of non-compliance leading to the urgency of the situation as described above.
312. In this case, the EDPB considers that the national decision needs to be adopted by the IE SA without undue delay and at the **latest by two weeks after the EDPB has notified its urgent binding decision to the IE SA and to all the CSAs**. The EDPB highlights, in this regard, that adopting the national decision prior to the expiry of the Provisional Measures on 3 November 2023 would be desirable as it would allow avoiding a gap in the legal situation for what concerns the Norwegian territory. Additionally, the IE SA will have to notify the national decision to Meta IE, attaching the urgent binding decision⁵⁵³.
313. The EDPB also requests the NO SA to inform Facebook Norway about the outcome of these proceedings, by sharing a copy of the national decision of the IE SA and of the urgent binding decision, following the notification by the IE SA of its national decision to Meta IE.

6 URGENT BINDING DECISION

314. In light of the above and in accordance with the tasks of the EDPB under Article 70(1)(t) GDPR to issue urgent binding decisions pursuant to Article 66 GDPR, the Board issues the following binding decision in accordance with Article 66(2) GDPR.
315. As regards the existence of infringements, based on the evidence provided, the EDPB concludes that there is an ongoing infringement of Article 6(1) GDPR arising from inappropriate reliance on Article 6(1)(b) GDPR for processing of personal data, including location data and advertisement interaction data, collected on Meta's products for behavioural advertising purposes.
316. The EDPB also concludes that there is an ongoing infringement of Article 6(1) GDPR arising from inappropriate reliance on Article 6(1)(f) GDPR for processing personal data collected on Meta's products for behavioural advertising purposes.
317. In addition, the EDPB concludes that Meta IE is currently in breach of its duty to comply with decisions by supervisory authorities.

⁵⁵¹ See Art. 65(6) GDPR.

⁵⁵² The IE SA considers the NO SA Request to the EDPB seeks to obtain an urgent binding decision from the EDPB, '*the net effect of which would be to compel the [IE SA], as LSA, to impose an EEA-wide ban (...)* (*In that regard, it is of course the case that it is not open to the EDPB to exercise corrective powers directly as against any controller or processor*)'. Letter from the IE SA to the NO SA of 13 October 2023, p. 3.

⁵⁵³ As described in Art. 65(6) GDPR and paragraph 308 above.

318. On the existence of urgency, the EDPB considers that, the urgent need to order final measures is clear in light of the risks that the infringements represent for the rights and freedoms of the data subjects without the adoption of final measures⁵⁵⁴. Because of such risks, the EDPB also finds that there is a need to derogate from the regular cooperation and consistency mechanisms to order final measures due to the urgency of the situation⁵⁵⁵.
319. The EDPB also considers that the IE SA, by not providing the information referred in Article 61(5) GDPR within the one-month deadline, failed to address the NO SA Mutual Assistance Request and that the presumption of urgency set by Article 61(8) GDPR is therefore applicable in this specific case, which further corroborates the need to derogate from the regular cooperation and consistency mechanisms⁵⁵⁶.
320. Considering the existence of the aforementioned ongoing infringements of the GDPR and the existence of an urgent need to act despite the ongoing process led by the IE SA, the EDPB considers that, at this point of time, further enforcement measures are necessary.
321. Therefore, in light of the analysis carried out above⁵⁵⁷ the EDPB considers it appropriate, proportionate and necessary to order final measures, consisting in a ban on processing pursuant to Article 58(2)(f) GDPR.
322. This ban on processing should be addressed to Meta IE, and become effective one week after the notification of the final measures to them.
323. The EDPB considers that the ban should refer to Meta IE's processing of personal data collected on Meta's products for behavioural advertising purposes on the basis of Article 6(1)(b) GDPR and Article 6(1)(f) GDPR across the entire EEA. The processing activities to which the ban refers are: (i) the processing of personal data, including location data and advertisement interaction data, collected on Meta's products for behavioural advertising purposes, having established in this respect the infringement of Article 6(1) GDPR arising from inappropriate reliance on Article 6(1)(b) GDPR; (ii) processing of personal data collected on Meta's products for behavioural advertising purposes, having ascertained in this respect the infringement of Article 6(1) GDPR arising from inappropriate reliance on Article 6(1)(f) GDPR.
324. The EDPB instructs the IE SA to adopt a national decision containing the final measures ordered by the EDPB without undue delay and at the latest by two weeks after the EDPB has notified its urgent binding decision to the IE SA and to all the CSAs. The IE SA shall notify the national decision, attaching the urgent binding decision of the EDPB, to Meta IE without undue delay.
325. The EDPB instructs the NO SA to inform Facebook Norway about the outcome of these proceedings.

7 FINAL REMARKS

326. This urgent binding decision is addressed to the IE SA, the NO SA and all the other CSAs.
327. The EDPB considers that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties.

⁵⁵⁴ See section 4.2.1.3 above.

⁵⁵⁵ See paragraph 220 above.

⁵⁵⁶ See section 4.2.2.3 above, including paragraph 257.

⁵⁵⁷ See Sections 5.1.3 and 5.1.4 above.

328. The IE SA shall adopt its national decision no later than two weeks after notification of the EDPB urgent binding decision.
329. The IE SA shall notify its national decision and this urgent binding decision to Meta IE without undue delay. The IE SA shall inform the EDPB of the date when the national decision is notified to the controller.
330. The NO SA shall inform Facebook Norway of the outcome of these proceedings without undue delay after the notification of the national decision to Meta IE.
331. The IE SA will communicate its final decision to the EDPB. Pursuant to Article 70(1)(y) GDPR, the IE SA's final decision communicated to the EDPB will be included in the register of decisions that have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)



EDPB Work Programme 2023/2024

Adopted on 14 February 2023

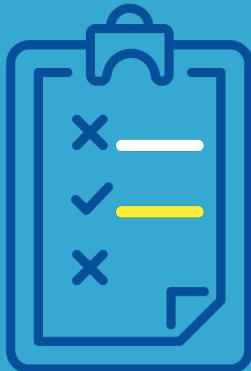
The European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body established by the General Data Protection Regulation (GDPR).

The EDPB has the following main tasks:

-  To issue opinions, guidelines, recommendations and best practices to promote a common understanding of the GDPR and the Law Enforcement Directive (LED);
-  To advise the European Commission on any issue related to the protection of personal data in the Union;
-  To contribute to the consistent application of the GDPR, in particular in cross-border data protection cases; and
-  To promote cooperation and the effective exchange of information and best practices between national supervisory authorities.

In line with the Article 29 of the EDPB Rules of procedure, the EDPB has developed its two-year work programme for 2023 and 2024, based on the EDPB Strategy and the needs identified by the members as priority for stakeholders.



Pillar I - Advancing harmonisation and facilitating compliance

As mentioned in the EDPB Strategy, in addition to providing practical and accessible guidance, the EDPB will develop and promote tools that help to implement data protection in practice, taking into account practical experiences of different stakeholders on the ground. Efforts will also go to make proactive use of the consistency mechanism, as well as of other tools in order to address potential divergences in the application of the GDPR.

- **Further guidance on key notions of EU data protection law**, developed also taking into account practical experience of stakeholders, gathered through stakeholder events and consultation



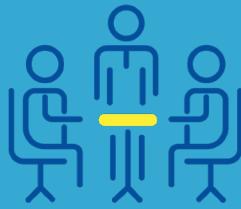
- ✓ Guidelines on data subject rights - right of access^{*}
- ✓ Targeted update of the Guidelines on identifying a controller or processor's lead supervisory authority*
- ✓ Targeted update on the Guidelines on Data Breach Notification*
- ✓ Guidelines on the use of Technologies for Detecting and Reporting Online Child Sexual Abuse
- ✓ Guidelines on legitimate interest
- ✓ Guidelines on children's data
- ✓ Guidelines on processing of data for medical and scientific research purposes
- ✓ Guidelines on the use of social media by public bodies

- **Consistency activities:** The EDPB will continue to take actions directly addressed to national supervisory authorities and which aim to ensure consistency of their decisions in a number of areas (e.g. evaluation of codes of conduct, certification schemes and criteria, binding corporate rules, creation of standard contractual clauses, lists of risky processing activities to be subject to a data protection impact assessment,...) in accordance with Article 64(1) and (2) GDPR. In addition, the EDPB will continue to act as a **dispute resolution body** in case of dispute between EEA supervisory authorities (Article 65 GDPR binding decisions; decisions/opinions in the context of an urgency procedure under Article 66 GDPR)
- Development and implementation of **compliance mechanisms** for controllers and processors (e.g. Guidelines on assessment of certification criteria *)
- **Advising the EU legislator on any important issue related to the protection of personal data** in the Union and intensifying engagement and cooperation with other regulators and policymakers (Digital euro, monitoring the legal developments relating to the digital package², etc.)
- **Development of awareness-raising common tools on the GDPR for a wider audience** (dedicated information for SMEs)

¹ The items accompanied by an asterisk (*) have already been adopted in their first version, but are to be finalised after public consultation.

² Digital Governance Act (Regulation 2022/868) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868>; Draft AI Act: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>; Draft Data Act: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN>; Digital Services Act (Regulation (EU) 2022/2065) <https://eur-lex.europa.eu/legal-content/en/EN/TXT/?uri=COM%3A2020%3A825%3AFIN>; Digital Markets Act (Regulation (EU) 2022/1925) <https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=O-1%3AL%3A2022%3A265%3ATOC&uri=uriserv%3AOJ.L..2022.265.01.0001.01.ENG>.

Pillar II - Supporting effective enforcement and efficient cooperation between national supervisory authorities



The EDPB will facilitate a more efficient functioning of the cooperation and consistency mechanism linking all national supervisory authorities, which work together to enforce European data protection law, by streamlining internal processes, combining expertise and promoting enhanced coordination. The EDPB will also strive to develop a genuine EU-wide enforcement culture among supervisory authorities. Therefore, it will actively endeavour to fulfil its role as a forum for the regular exchange of information on ongoing cases.

- Encouraging and facilitating the use of the **full range of cooperation tools** enshrined in Chapter VII of the GDPR and Chapter VII of the LED and continuously evaluating and improving the efficiency and effectiveness of these tools, as well as further promoting a common application of key concepts in the cooperation procedure



- ✓ Guidelines on administrative fines *
- ✓ Guidelines on Article 61 GDPR - Mutual assistance
- ✓ Guidelines on Article 66 GDPR
- ✓ Template for data subjects complaints
- ✓ Right to be heard and right of access to the file concerning cooperation procedures according to Article 60 GDPR

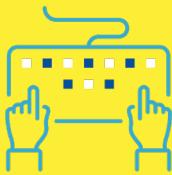
- Implementation of the **Coordinated Enforcement Framework** (CEF) to carry out annual coordinated actions on pre-defined topics to allow SAs to pursue joint actions in a flexible but coordinated manner: 2023 CEF on the designation and position of the data protection officer
- Support of the work on the **cases of strategic importance**
- Creation of **Task forces** when needed to provide an operational platform for cases requiring cooperation on enforcement matters
- Possible Opinion on EC draft legislation aiming to harmonise administrative laws of the GDPR enforcement
- Implementation of the **Support Pool of Experts** (SPE) to provide material support to EDPB Members in the form of expertise that is useful for investigations and enforcement activities, as a continuation of the pilot phase
- **Approval procedures** that require a cooperation phase among SAs, followed by an EDPB consistency action (Procedure for the approval of certification criteria, procedure for the approval of Ad-hoc Contractual Clauses (Article 46(3)(a) GDPR) and Standard Data Protection Clauses (Article 46(2)(d) GDPR), Procedure for the adoption of BCR)
- Deployment of the **EDPB secondment program** (staff exchanges), as a continuation of the pilot phase

Pillar III - A fundamental rights approach to new technologies



As mentioned in the EDPB Strategy, the EDPB will monitor new and emerging technologies and their potential impact on the fundamental rights and daily lives of individuals, and will help to shape Europe's digital future in line with our common values and rules, while continuing to work with other regulators and policymakers to promote regulatory coherence and enhanced protection for individuals.

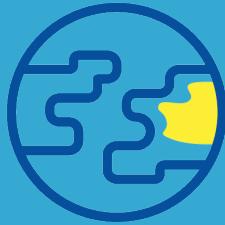
- Reinforcing the application of fundamental data protection principles and individual rights and establishing common positions and **guidance**, especially in the context of new technologies



- ✓ Guidelines on use of facial recognition by law enforcement authorities*
- ✓ Guidelines on Anonymisation
- ✓ Guidelines on Pseudonymisation
- ✓ Guidelines on Blockchain
- ✓ Guidelines on telemetry and diagnostic data
- ✓ Guidelines on the interplay between the AI Act and the GDPR

- Strengthening cooperation with **external stakeholders**

Pillar IV - The global dimension



As mentioned in the EDPB Strategy, the EDPB is determined to set and promote high EU and global standards for international data transfers to third countries and will reinforce its engagement with the international community to promote EU data protection as a global model and to ensure effective protection of personal data beyond the EU borders.

- Providing **guidance** on the use of transfer tools ensuring an essentially equivalent level of protection and increasing awareness on their practical implementation and issues relating to government access to personal data



- ✓ Opinions on and review of adequacy decisions (US, Japan etc.)
- ✓ Referential for the approval of BCR Controller *
- ✓ Referential for the approval of BCR Processor
- ✓ Guidance on Article 48 GDPR
- ✓ Guidelines on Article 37 LED

- Engaging with the **international community** to promote EU data protection as a global model and to ensure effective protection of personal data beyond EU borders
- Facilitating the engagement between EDPB members and the supervisory authorities of **third countries** with a focus on **cooperation** in enforcement cases involving controllers/ processors located outside the EEA

Annex - Documents already adopted in early 2023

- ✓ Report of the work undertaken by the Cookie Banner Taskforce (adopted on 17 January 2023)
- ✓ 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector (adopted on 17 January 2023)
- ✓ Guidelines on deceptive design patterns in social media platform interfaces: How to recognise and avoid them (finalised after public consultation on 14 February 2023)
- ✓ Guidelines on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (finalised after public consultation on 14 February 2023)
- ✓ Guidelines on certification as a tool for transfers (finalised after public consultation on 14 February 2023)
- ✓ Procedure for the adoption of the EDPB Opinions regarding national criteria for certification and European Data Protection Seals (adopted on 14 February 2023)

EDPB Work Programme 2024–2025



Adopted on 8 October 2024

The European Data Protection Board (EDPB) is an independent European body established by the General Data Protection Regulation (GDPR).

The EDPB has the following main tasks:

- To issue opinions, guidelines, recommendations and best practices to promote a common understanding of the GDPR and the Law Enforcement Directive (LED);
- To advise the European Commission on any issue related to the protection of personal data in the Union;
- To contribute to the consistent application of the GDPR, in particular in cross-border data protection cases; and
- To promote cooperation and the effective exchange of information and best practices between national supervisory authorities.

The EDPB has developed a new work programme for 2024 and 2025¹, the first of two which will implement the EDPB Strategy for 2024–2027². It is based on the priorities set out in the EDPB Strategy, and the needs identified by the members as most important for stakeholders.

1. In line with the Article 29 of the EDPB Rules of Procedure. This Work Programme is valid from 8 October 2024 until 31 December 2025 and supersedes, for the remaining part of 2024, the previous Work Programme 2023–2024.

2. https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf

Enhancing harmonisation and promoting compliance



The EDPB will continue to provide concise, practical and clear guidance that is accessible to the relevant audience. In addition, the EDPB will develop and promote tools for a wider audience and produce content that is accessible for non-experts, SMEs and individuals, including particularly vulnerable data subjects such as children. As a further element to pursue a consistent application and implementation of data protection law, the EDPB will continue supporting the development of compliance measures, including through the engagement with stakeholders. The EDPB will also continue to assess how personal data are being accessed and used by public authorities for law-enforcement purposes.

KEY ACTION 1

Developing further guidance on key issues and concepts of EU data protection law, taking into account the practical experience of stakeholders as gathered through stakeholder events and consultation. This guidance will cover a number of topics, including:

- Guidelines on anonymisation
- Guidelines on pseudonymisation
- Guidelines on legitimate interest*
- Guidelines on children's data
- Guidelines on "consent or pay" models
- Guidelines on the processing of data for scientific research purposes
- Guidelines on data subject rights under the LED – right of access
- Follow-up on the implications of Judgment of the Court of Justice of the European Union (CJEU) on Passenger Names Records (PNR)³
- Document on Age verification criteria

KEY ACTION 2

Further develop information streams for a wider audience to complement the EDPB's technical and legally-focused publications (for non-experts and individuals, including children). These may include factsheets which communicate a guideline's core message in an accessible way, further improvements and promotion of the EDPB Data Protection Guide for Small Businesses⁴, and other templates and checklists.

3. CJEU judgment of 21 June 2022 C-817/19 Ligue des droits humains, regarding the implementation of the Directive (EU) 2016/681 on the use of PNR in Member States (ECLI:EU:C:2022:491).

4. https://www.edpb.europa.eu/sme-data-protection-guide/home_en

*. These guidelines were already adopted in their version for public consultation at the October plenary meeting.

KEY ACTION 3

Support the development and implementation of compliance measures for controllers and processors, including:

✓ Issuing opinions on:

- accreditation requirements for monitoring bodies of codes of conduct and for certification bodies
- codes of conduct⁵ and on certification criteria⁶, including the European Data Protection Seal)

✓ Engaging with stakeholders on compliance measures, including:

- collaboration concerning certification mechanisms pursuant to the GDPR
- cooperation on cybersecurity certification schemes
- interaction with key groups of stakeholders to raise awareness and foster their understanding, for example, of how certification and codes of conduct can be used

KEY ACTION 4

Advise the EU legislature on any important issue related to the protection of personal data in the Union

5. Under Article 40(7) GDPR

6. Under Article 45(2) GDPR

Reinforcing a common enforcement culture and effective cooperation



The EDPB will further strengthen efforts to ensure effective enforcement of the GDPR and cooperation between the members of the EDPB, building on its commitments made in the Vienna statement on enforcement cooperation and on the opportunities arising from the future Regulation on GDPR procedural rules. The EDPB will actively endeavour to fulfil its role as a forum for the regular exchange of information on ongoing cases, as well as continuing to support the development of cooperation and enforcement tools, and the sharing of expertise. Efforts will also go to ensure the smooth functioning of the consistency mechanism.

KEY ACTION 1

Encourage and facilitate the use of the full range of cooperation tools enshrined in Chapter VII of the GDPR and Chapter VII of the LED, continuously evaluating and improving the efficiency and effectiveness of these tools, and further promoting a common application of key concepts in the cooperation procedure. This will also include guidance and work on a number of topics, including:

- Advice to the co-legislators on the Proposal on GDPR procedural rules and preparation of the groundwork aimed to effectively apply the future regulation
- Guidelines on Article 61 GDPR – Mutual assistance
- Guidelines on Article 66 GDPR – Urgency procedure
- Update of the EDPB endorsed Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of the GDPR
- Development of commonly understood notions to enable a consistent and comparable reporting of enforcement activities and facilitate statistics
- Assess the need to update the Internal EDPB Document 1/2021 on the application of Article 62 GDPR – Joint Operations

KEY ACTION 2

Support enforcement and the exchanges of information and best practices, including:

- Implementing the Coordinated Enforcement Framework (CEF), including:
 - The 2024 CEF on the implementation of the right of access by controllers
 - A fourth coordinated action to be launched in 2025, on a topic to be determined once the third action is completed
- Fostering identification of strategic cases for which cooperation will be prioritised
- Creating task forces, when needed, to provide operational platforms for cases requiring cooperation on enforcement matters
- Continuing to develop and implement various actions and projects undertaken under the Support Pool of Experts to provide material support to EDPB Members and to coordinate

- exchanges between EDPB members on enforcement and inspection methodologies
- Continuing to develop EDPB secondment programme for staff exchanges between EDPB members
 - Organising trainings and workshops for EDPB members, such as on Certification, Binding corporate rules or on enforcement matters

KEY ACTION 3

Ensure a robust functioning of the consistency mechanism, including by:

- Continuing to adopt opinions under Article 64(1) and (2) GDPR that are directly addressed to national supervisory authorities and which aim to ensure consistency of their decisions
- Continuing to act as a dispute resolution body in disputes between EEA supervisory authorities (Article 65 GDPR binding decisions) and by adopting decisions/opinions in the context of urgency procedures under Article 66 GDPR
- Taking actions to ensure the application of the future Regulation on GDPR procedural rules insofar as those rules concern the consistency mechanism

KEY ACTION 4

Evaluate and enhance the IT tools and systems used by the EDPB, including by:

- Exchanging and reviewing best practices in the use of the Internal Market Information system (IMI)
- Developing an application to monitor GDPR procedures in IMI, and to automate statistics and report generation by connecting to the existing IMI system's API
- Evaluating and enhancing IT solutions provided by the EDPB Secretariat

Safeguarding data protection in the developing digital and cross-regulatory landscape



The EDPB will promote a consistent application of different regulatory frameworks and cooperation with other regulatory authorities in the developing cross-regulatory and interdisciplinary landscape. The EDPB will also continue to promote a human-centric approach to new technologies.

KEY ACTION 1

Continue to take an active role in relevant forums, including the DMA High Level Group and the European Data Innovation Board.

KEY ACTION 2

Establish common positions and guidance in the cross-regulatory landscape on topics including:

- Guidelines on the interplays between EU data protection law and other EU laws, including separate guidelines for each of the AI Act, the Digital Services Act, the Digital Markets Act
- Position paper on the interplay between EU data protection and competition law
- Guidelines on the processing of personal data to target or deliver political advertisements
- Guidelines on transfers of personal data in the context of transfers of crypto assets
- Document concerning anti-money laundering and countering financing of terrorism (AML/CFT) requirements, in particular on the information service providers used by obliged entities in the context of the performance of their obligations in such sector.

KEY ACTION 3

Cooperate with other regulatory authorities on matters relating to data protection, including competition authorities, consumer protection authorities and authorities competent under other legal acts.

KEY ACTION 4

Monitor and assess new technologies, with the development of guidance to promote a human-centric approach to topics including:

- Guidelines on generative AI – data scraping
- Document on the mandatory user accounts on online shopping websites
- Guidelines on telemetry and diagnostic data
- Guidelines on blockchain
- Guidelines on the use of social media by public bodies

KEY ACTION 5

Engage and cooperate with the EU legislators and with other EU institutions and bodies, including by reacting, where appropriate, to developments relating to the digital euro and the financial data access and payments package.

PILLAR 4

Contributing to the global dialogue on data protection



The EDPB will continue to promote a global dialogue on privacy and data protection, including a focus on the international community supporting cooperation on enforcement between EU and non-EU authorities. The EDPB will also continue working on GDPR and LED transfer mechanisms.

KEY ACTION 1

Continue to work on the GDPR and LED data transfer mechanisms and provide further guidance on their practical implementation. This will include:

- Opinions on and review of adequacy decisions
- Opinions on administrative arrangements
- Opinions on Binding Corporate Rules and streamlining the approval process
- Opinions on certification as a tool for transfers
- Opinions on standard contractual clauses and ad-hoc contractual clauses
- Guidelines on Article 48 GDPR
- Update of Referential for BCR Processor

KEY ACTION 2

Support the exchange of information and cooperation among EDPB members active in international forums and continuing to engage with the international community to promote high data protection standards.

KEY ACTION 3

Facilitate and strengthen cooperation between EDPB members and non-EU authorities, increasing efforts related to the EDPB's contributions on international cooperation and supporting enforcement.



European Data Protection Board

EDPB Work Programme 2021/2022

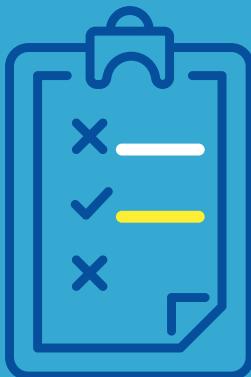
The European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body established by the General Data Protection Regulation (GDPR).

The EDPB has the following main tasks:

-  To issue opinions, guidelines, recommendations and best practices to promote a common understanding of the GDPR and the Law Enforcement Directive (LED);
-  To advise the European Commission on any issue related to the protection of personal data in the Union;
-  To contribute to the consistent application of the GDPR, in particular in cross-border data protection cases; and
-  To promote cooperation and the effective exchange of information and best practices between national supervisory authorities.

In line with the Article 29 of the EDPB Rules of procedure, the EDPB has developed its two-year work programme for 2021 and 2022, based on the EDPB Strategy 2021-2023 and the needs identified by the members as priority for stakeholders.



Pillar I - Advancing harmonisation and facilitating compliance

As mentioned in the EDPB Strategy, in addition to providing practical and accessible guidance, the EDPB will develop and promote tools that help to implement data protection in practice, taking into account practical experiences of different stakeholders on the ground. Efforts will also go to make proactive use of the consistency mechanism, as well as of other tools in order to address potential divergences in the application of the GDPR.

- **Further guidance on key notions of EU data protection law, developed also taking into account practical experience of stakeholders, gathered through stakeholder events and consultations**



- ✓ [Guidelines on controller and processor*](#)¹
- ✓ [Guidelines on Article 23 GDPR*](#)
- ✓ [Guidelines on the targeting of social media users*](#)
- ✓ Guidelines on data subject rights
- ✓ Guidelines on legitimate interest
- ✓ Guidelines on processing of personal data for medical and scientific research purposes
- ✓ Guidelines on children's data
- ✓ Guidance on remuneration against personal data

- **Consistency activities:** The EDPB will continue to take actions directly addressed to national supervisory authorities and which aim to ensure consistency of their decisions in a number of areas (e.g. evaluation of codes of conduct, certification schemes and criteria, binding corporate rules, creation of standard contractual clauses, lists of risky processing activities to be subject to a data protection impact assessment,...) in accordance with Article 64(1) and (2) GDPR. In addition, the EDPB will continue to act as a dispute resolution body in case of dispute between EEA supervisory authorities (Article 65(1) GDPR binding decisions; decisions/opinions in the context of an urgency procedure under Article 66 GDPR).
- **Development and implementation of compliance mechanisms for controllers and processors** (e.g. Guidelines on assessment of certification criteria)
- **Advising the EU legislator on any important issue related to the protection of personal data in the Union** (e.g. Data Governance Act, ePrivacy, Anti-Money Laundering legislation, etc.)², and intensifying engagement and cooperation with other regulators and policymakers
- **Development of awareness-raising common tools on the GDPR for a wider audience** (e.g., tools specifically tailored for non-expert professionals, such as SMEs and data subjects)

¹ The items accompanied by an asterisk (*) have already been adopted in their first version, but are to be finalised after public consultation.

² Either on the EDPB's own initiative or upon request, for instance from the European Commission. For EDPB opinions on adequacy decisions, see Pillar IV below.

Pillar II - Supporting effective enforcement and efficient cooperation between national supervisory authorities



The EDPB will facilitate a more efficient functioning of the cooperation and consistency mechanism linking all national supervisory authorities, which work together to enforce European data protection law, by streamlining internal processes, combining expertise and promoting enhanced coordination. The EDPB will also strive to develop a genuine EU-wide enforcement culture among supervisory authorities. Therefore, it will actively endeavour to fulfil its role as a forum for the regular exchange of information on ongoing cases.

- **Encouraging and facilitating the use of the full range of cooperation tools enshrined in Chapter VII of the GDPR and Chapter VII of the LED and continuously evaluating and improving the efficiency and effectiveness of these tools, as well as further promoting a common application of key concepts in the cooperation procedure**

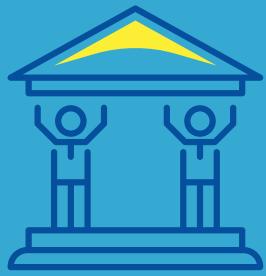


- ✓ Guidance on Art. 60 GDPR – One-stop-shop
- ✓ Guidance on Art. 61 GDPR – Mutual assistance
- ✓ Guidelines on Article 65 GDPR
- ✓ Guidelines on the calculation of administrative fines
- ✓ Assessment of the practical implementation of the amicable settlement

- **Implementation of the Coordinated Enforcement Framework (CEF)³** to carry out annual coordinated actions on pre-defined topics to allow SAs to pursue joint actions in a flexible but coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations.
- **Implementation of the Support Pool of Experts (SPE)⁴**: the EDPB will launch the SPE pilot project 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.

³ EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 (https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/edpb-document-coordinated-enforcement-framework-under-regulation_en).

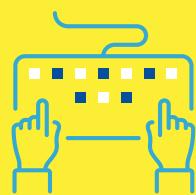
⁴ EDPB Document on Terms of Reference of the EDPB Support Pool of Experts (https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-terms-reference-edpb-support-pool-experts_en).



Pillar III - A fundamental rights approach to new technologies

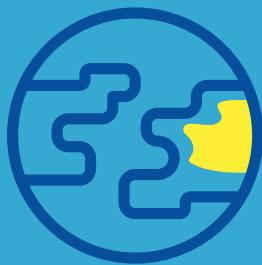
As mentioned in the EDPB Strategy, the EDPB will monitor new and emerging technologies and their potential impact on the fundamental rights and daily lives of individuals, and will help to shape Europe's digital future in line with our common values and rules, while continuing to work with other regulators and policymakers to promote regulatory coherence and enhanced protection for individuals.

- **Reinforcing the application of fundamental data protection principles and individual rights and establishing common positions and guidance, especially in the context of new technologies**



- ✓ [Guidelines on examples regarding Data breach notifications*](#)
- ✓ [Guidelines on Blockchain](#)
- ✓ [Guidelines on Anonymisation and Pseudonymisation](#)
- ✓ [Guidelines on the use of facial recognition technology in the area of law enforcement](#)
- ✓ [Guidelines on virtual voice assistants*](#)
- ✓ [Guidelines on data protection in social media platform interfaces: practical recommendations](#)
- ✓ Any additional guidance on legal implications relating to technological issues, such as Cloud computing, Artificial intelligence/Machine Learning, Digital Identity & Identity Federation, Data Brokers, Internet of Things, and payment methods

- **Strengthening cooperation with external stakeholders** (ENISA advisory group, ISO liaison, Contact point of the Stakeholder Cybersecurity Certification Group, etc.)



Pillar IV - The global dimension

As mentioned in the EDPB Strategy, the EDPB is determined to set and promote high EU and global standards for international data transfers to third countries and will reinforce its engagement with the international community to promote EU data protection as a global model and to ensure effective protection of personal data beyond the EU borders.

- **Providing guidance on the use of transfer tools ensuring an essentially equivalent level of protection and increasing awareness on their practical implementation and issues relating to government access to personal data**



- ✓ Recommendations on supplementary measures (on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data)*
- ✓ Opinions on and review of adequacy decisions (UK, Republic of Korea, review of Japan decision, any revision of 95/46 adequacy decisions...) PNR agreements (UK, Canada, Japan...)
- ✓ Guidelines on codes of conduct as a tool for international transfers
- ✓ Guidelines on certification as a tool for international transfers
- ✓ Guidelines on Article 37 LED (transfers subject to appropriate safeguards)
- ✓ Guidance on Article 48 GDPR (transfers or disclosures not authorised by Union law)
- ✓ Territorial scope (Article 3) of the GDPR and its interplay with Chapter V
- ✓ Statement on the proposed second additional protocol to the Council of Europe Convention on Cybercrime
- ✓ International agreements involving transfers, including FATCA and OECD CRS
- ✓ Approval procedure for Article 46.3(a) ad-hoc contractual clauses and Article 46.2(d) GDPR standard data protection clauses

- **Engaging with the international community to promote EU data protection as a global model and to ensure effective protection of personal data beyond EU borders**

- **Facilitating the engagement between EDPB members and the supervisory authorities of third countries with a focus on cooperation in enforcement cases involving controllers/processors located outside the EEA**

Annex - Documents already adopted in early 2021

- ✓ Statement on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)
- ✓ Recommendations on the adequacy referential under the Law Enforcement Directive
- ✓ EDPB Document on the response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research
- ✓ EDPB-EDPS Joint Opinion on Standard contractual clauses between controllers and processors
- ✓ EDPB-EDPS Joint Opinion on Standard contractual clauses for the transfer of personal data to third countries
- ✓ Guidelines on relevant and reasoned objection under Regulation 2016/679
- ✓ Guidelines on processing personal data in the context of connected vehicles and mobility related applications
- ✓ EDPB-EDPS Joint Opinion on Standard contractual clauses for the transfer of personal data to third countries
- ✓ Guidelines on relevant and reasoned objection under Regulation 2016/679
- ✓ Guidelines on processing personal data in the context of connected vehicles and mobility related applications

EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)

Brussels, 13th November 2019

Preliminary remarks and context of the EDPB contribution

The European Data Protection Board (EDPB) very much welcomes the opportunity of the consultation held by the Council of Europe Cybercrime Convention Committee (T-CY) on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention). Such consultation process is even more essential considering that the meetings dedicated to the preparation of the additional protocol are being held in closed sessions and that the direct involvement of data protection authorities in the drafting process has not been foreseen in the T-CY Terms of Reference¹. The EDPB therefore wishes to provide a constructive and objective contribution with a view to ensure that data protection consideration are duly taken into account in the overall drafting process of the additional protocol.

Access to personal data across jurisdictions has already been addressed in the past by EU data protection authorities in various positions and opinions and the EDPB wishes to recall in particular the Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime², as well

¹ Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, Approved by the 17th Plenary of the T-CY on 8 June 2017, T-CY (2017)3: <https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b>

² Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, 05/12/2013: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf

as its statement on data protection and privacy aspects of cross-border access to electronic evidence³. The European Data Protection Supervisor issued Opinion 03/2019 on the mandate for the participation of the Commission in the negotiations⁴, as well as Opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters⁵. This contribution also builds upon the EDPB Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters⁶.

The EDPB acknowledges that situations where judicial and law enforcement authorities are faced with a “cross-border situation” with regards to access to personal data as part of their investigations can be a challenging reality and recognises the legitimate objective of enhancing international cooperation on cybercrime and access to information. In parallel, the EDPB recalls that the protection of personal data and legal certainty must be guaranteed, thus contributing to the objective of 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. The EDPB furthermore shares the objective of enshrining the preparation of the additional protocol within the framework of the Council of Europe core values and principles, and in particular human rights and the rule of law.

With regards to trans-border direct access to stored computer data as per Article 32(b) of the Budapest Convention, the EDPB reaffirms in particular that data controller can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required.

As the Cybercrime Convention, as well as any of its additional protocols, is to be considered as a binding international instrument, the EDPB stresses that, in line with the CJEU case law, the “obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness⁷. It is therefore essential that EU negotiating parties ensure that the provisions laid down in the additional protocol do comply with the EU *acquis* in the field of data protection in order to ensure its compatibility with EU primary and secondary law.

³ WP29 statement on data protection and privacy aspects of cross-border access to electronic evidence, 29 November 2017: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610177

⁴ EDPS opinion 3/19 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention: https://edps.europa.eu/data-protection/our-work/publications/opinions/budapest-cybercrime-convention_en

⁵ EDPS opinion 7/19 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters: https://edps.europa.eu/data-protection/our-work/publications/opinions/electronic-evidence-criminal-matters_en

⁶ Opinion 23/2018 of the EDPB adopted on 26 September 2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters: https://edpb.europa.eu/our-work-tools/our-documents/opinia-art-70/opinion-232018-commission-proposals-european-production_en

⁷ See CJEU joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461 - par (285).

Considering the timeframe of the consultation process, this EDPB contribution will focus on a preliminary assessment of the provisional texts published on 1st October and in particular the new provisions on direct disclosure of subscriber information and on the giving effect to orders from another Party for expedited production of data. The EDPB understands that dedicated provisions on the protection of personal data are still being discussed and will, in this regard, lay down a series of initial recommendations to be considered by the T-CY. As for previous provisions, the EDPB remains available for further contributions and calls for an early and more proactive involvement of data protection authorities in the preparation of these specific provisions, in order to ensure an optimal understanding and consideration of data protections safeguards.

Provisional text of provisions on direct disclosure of subscriber information and on the giving effect of orders for expedited production of data

The EDPB particularly welcomes the opportunity to comment on the draft procedure that provides for the direct cooperation between the authorities of one Party and a service provider in the territory of another Party to obtain subscriber information, as well as on the ability for the requested party to give effect to received order by compelling a service provider in its territory to produce subscriber information or traffic data in the service provider's possession or control. While such provisions may appear of a mainly procedural nature, they are essential in determining the conditions for access to personal data and therefore in assessing a possible interference with the right to the protection of personal data as guaranteed by Article 7 of the Charter of Fundamental Rights of the Union. On the basis of its preliminary assessment, the EDPB recommends further examining the draft provisions with regard to the following elements.

Systematic involvement of judicial authorities of the requested party

The EDPB welcomes the possibility, as per Article 4(5), for a Party to require that an order issued to a service provider in its territory is simultaneously notified to its authorities and that the designated authority may instruct the service provider not to disclose the information if conditions or grounds for refusal would apply under Articles 25.4 and 27.4 of the Convention. However, such safeguard remains at the discretion of each Party to the Convention. As far as EU Parties are concerned, the EDPB stresses that safeguards and limitations affecting the procedural conditions for access to personal data will have to be applied consistently in order to ensure a harmonised level of protection for all persons in the Union.

Article 4(5) does not specifically mention to which type of authority in the requested State orders are to be notified and possibly reviewed. The EDPB recommends that further requirements are included in order to ensure that judicial authorities designated by the authorities of the service provider are involved as early as possible in the process of gathering subscriber information in order to give these authorities the possibility to effectively review compliance of the orders with the Convention and ensure the obligation for these authorities

to raise grounds for refusal on that basis. In this regard, the EDPB recalls that in its case law concerning access to communications data for law enforcement purposes, the CJEU has restricted the possibility to provide for such access, among other criteria, and “except in cases of validly established urgency”⁸, to a “prior review carried out by a court or an independent administrative body”, “following a reasoned request of [competent national] authorities submitted within the framework of procedures of prevention, detection or criminal prosecution.”⁹

The systematic involvement of judicial authorities in the requested parties is also essential to preserve the application of the principle of dual criminality in the field of judicial cooperation. The EDPB recalls that the dual criminality principle aims at providing an additional safeguard to ensure that a State cannot rely on the assistance of another to apply a criminal sanction which does not exist in the law of another State.

Limitation to the status of requesting authority

The EDPB notes and welcomes that, according to Article 4, paragraph 2b, only the requested Party, via a declaration, can impose that the requesting authority is a prosecutor, a judicial authority or another independent authority. However, this could imply, *a contrario* and in the absence of such declaration, that where the requested State did not make such a declaration, orders to service providers could be issued by any authority in the requesting Party. Due to the direct effect of the additional protocol to the Convention in the EU legal order, the draft provisions could then be interpreted as allowing any authority to issue an order, thus putting the lawfulness of the agreement into question in light of EU law. In light of the CJEU case law already cited, the EDPB considers that the type of requesting authorities who may issue such order should be limited to prosecutor, a judicial authority or another independent authority.

Categories of data, definition of “subscriber information” and type of offence

The EDPB recommends that the definition of subscriber information, as per Article 18.3 of the Convention, be further clarified in order to avoid inclusion of any traffic data or content data. Information needed for the purpose of identifying a subscriber of a service may indeed include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time, which under EU law constitute traffic data relating to the transmission of a communication. In addition, the EDPB recalls that, in accordance with the relevant CJEU case law, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way. The CJEU has furthermore ruled in its judgement in joined cases C-203/15 and C-698/15 Tele2 Sverige AB that metadata such as traffic data and location data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications¹⁰.

⁸ See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (120)

⁹ See CJEU joint cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238 – par (62)

¹⁰ See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (99)

The EDPB also takes the view that the balance between the types of offences for which an Order can be issued and the categories of data concerned shall be reassessed in order to limit the possibility to submit an Order to produce data that could be considered as traffic data, to serious crimes only. Furthermore, the definition of a common list of specific serious criminal offences should be further explored.

Security of data processing

Although Article 4(6) and Article 5(5) provide that appropriate levels of security and authentication may be required, the EDPB encourages the development of further specifications and requirements in this regard. Ensuring that the necessary means are put in place so that the personal data are disclosed and communicated in a secure environment with the means to ensure the authenticity of documents is key for achieving the objective of a swift gathering of electronic evidence in compliance with fundamental rights.

In relation to the security of data processing, the EDPB also invites the T-CY to consider, as a specific data protection safeguard, a mechanism for the notification without delay of data breaches that could seriously interfere with the rights and freedoms of data subjects. Personal data breaches could indeed potentially have a range of significant adverse effects for individuals concerned.

Provisions on data protection safeguards

The EDPB considers essential that the provisional text submitted to public consultation is complemented by dedicated provisions on data protection safeguards, which must then be assessed together in order to ensure the draft additional protocol translates into a sustainable arrangement for the sharing of personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights.

Provisional text of provisions on direct disclosure of subscriber information and on the giving effect to orders from another Party for expedited production of data, by laying down procedural conditions for access to personal data, may already impact on the level of protection of personal data and may also need to be amended in order to ensure the operational application of appropriate data protection safeguards.

The EDPB considers that specific provisions on data protection safeguards shall reflect key principles and in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. These principles are also in line with the Council of Europe modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), to which many Parties to the Convention on Cybercrime are also Party.

Substantive and procedural conditions for access to personal data

As stated by the Article 29 Working Party on data protection and privacy aspects of cross-border access to electronic evidence, the EDPB recalls that the current EU legal framework and the most recent case law can allow the development of a list of substantive and

procedural conditions to be taken into account for any future instrument governing law enforcement access to personal data. Considering the direct effect of an additional protocol to the Convention in the EU legal order, the following conditions for access to personal data remain relevant:

- The conditions under which the providers of electronic communications services must grant such access must be provided by law, so as to ensure that the processing relies on a clear legal basis.
- Individual access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.
- Access of the competent national authorities to data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body.
- In particular situations, where for example national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.
- Personal data collected should be adequate, relevant and not excessive for the purpose of the processing.
- The processing of special categories of personal data should be subject to further limitations and safeguards.
- The competent national authorities to whom access to the data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities.
- Personal data should be correct, up to date and should not be kept longer than necessary.
- Notification is necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy and their data protection rights in relation to the processing of their data.

Availability of effective legal remedies

The EDPB also considers of paramount importance that the additional protocol includes mechanism to ensure the availability of legal remedies to the data subject whose data has been obtained, at least equivalent to those available in a domestic case. In this regard, the EDPB recalls that the CJEU has stated that “the first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law”¹¹.

¹¹ See CJEU C-362/14, Maximillian Schrems, ECLI:EU:C:2015:650 – par (95)

Further processing and onward transfer

The EDPB highlights that published provisional texts do not contain any specific limit with regard to the further processing and onward transfers of the transferred personal data by the requesting Party authority. The EDPB therefore recommends specifying narrowly the purposes of the transfers and the prohibition of further processing incompatible with those purposes and including the general principle of prohibition of onward transfers unless the third country provides an appropriate level of protection, in order to prevent the level of protection provided for in the protocol from being circumvented by further processing and onward transfers of personal data to other third countries.

Oversight and monitoring mechanism

In light of the comments and recommendations above, the EDPB finally invites the T-CY to consider the development of a mechanism for the oversight and monitoring by an independent authority, with both investigatory and corrective enforcement powers, responsible to ensure the application of future data protection safeguards in practice.

The EDPB reiterates the importance of involving data protection authorities in the drafting process of the additional protocol and stands ready to contribute and assist the T-CY in the preparation of provisional text of provisions on data protection safeguards.

Olivier Micol

Brussels, 14 April 2020

Head of Unit European Commission
DG for Justice and Consumers
Unit C.3 – Data protection
Belgium

Ref: OUT2020-0028

Dear M. Micol,

Thank you very much for liaising and seeking the advice of the EDPB on the draft Guidance on apps supporting the fight against COVID-19 pandemic. Indeed, the EDPB has been keen to work fast on this issue by publishing a statement on March 19th and plans to issue additional guidance next week on tracing, scientific research and teleworking. Some National Supervisory Authorities are also developing guidelines at national level to advise their governments and telecoms operators on the best way to comply with data protection rules. The EDPB welcomes the Commission's initiative in developing a pan-European and coordinated approach, where mobile applications may become one of the proposed measures to empower individuals in the response to fight the pandemic. The EDPB has repeatedly stated that the implementation of data protection principles and the respect of fundamental rights and freedoms is not only a legal obligation, but also a requirement to reinforce the effectiveness of any data-based initiatives for combating the spread of the COVID-19 virus and for informing de-escalation strategies.

The EDPB is aware that no one-size-fits-all solution applies to the matter at stake, and that the available options require many factors to be considered, including the fact that individuals' health may be impacted. This is why envisaged technical solutions need to be examined in detail, on a case-by-case basis. In addition, the EDPB believes that it is a step in the right direction to highlight the essential need to consult with data protection authorities to ensure that personal data is processed lawfully, respecting the rights of the individuals, in accordance with data protection law.

The development of the apps should be made in an accountable way, documenting with a data protection impact assessment all the implemented privacy by design and privacy by default mechanisms, and the source code should be made publicly available for the widest possible scrutiny by the scientific community.

At this stage, and on the basis of the information provided by the Commission, the EDPB can only focus on the overall goal of the envisaged apps, to verify whether they are in line with data protection principles, and on the mechanisms provided for the exercise of the rights and freedoms of the population. Doing so, the EDPB believes that the Commission will draw elements for a further reflection in order to adjust, where needed, the choices represented in the document, or to explore

new technical options. In any case, the EDPB will investigate further this issue in its upcoming guidelines.

In this answer, the EDPB would like to address specifically the use of apps for the contact tracing and warning functionality, because this is where increased attention must be paid in order to minimise interferences with private life while still allowing data processing with the goal of preserving public health.

In the case where such applications would prove relevant in the implementation of some public health policy, they may only achieve their maximum efficiency if used by the largest possible share of the population, in a collective effort to fight the virus. Any functional heterogeneity, lack of interoperability or even individual difference in the use of the app may create negative externalities on others, resulting in a reduced sanitary effect. The EDPB strongly supports the Commission's proposal for a voluntary adoption of such apps, a choice that should be made by individuals as a token of collective responsibility. It should be pointed out that voluntary adoption is associated with individual trust, thus further illustrating the importance of data protection principles.

The EDPB notes that the mere fact that the use of the contact tracing takes place on a voluntary basis, does not mean that the processing of personal data by public authorities necessarily be based on the consent. When public authorities provide a service, based on a mandate assigned by and in line with requirements laid down in law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task for public interest. The enactment of national laws, promoting the voluntary use of the app without any negative consequence for the individuals not using it, could be a legal basis for the use of the apps. Such legislative interventions should accordingly not be intended as a means to push for compulsory adoption, and the individuals should be free to install and uninstall the app at will. These laws could be accompanied by appropriate communications activities at national level to promote such tools, with awareness-raising campaigns and assistance to minors, to the impaired, or to less skilled or educated parts of the population, in order to avoid scattered adoption, or blurred knowledge of the evolution of the epidemics and any potential health divide. Indeed, any lack of data, due to individuals' inattentive use of the app or even to battery fault of the device may seriously undermine the overall public usefulness of these instruments.

Contact tracing apps do not require location tracking of individuals users. Their goal is not to follow the movements of individuals or to enforce prescriptions. The main function of such apps is to discover events (contacts with positive persons), which are only likely and for the majority of users may not even happen, especially in the de-escalation phase. Collecting an individual's movements in the context of contact tracing apps would violate the principle of data minimisation. In addition, doing so would create major security and privacy risks.

Health authorities and scientists are well placed to identify what constitutes an event to be shared if, where and when it happens, under a strict necessity test as required by the law, and they should define some of the functional requirements of the app. Another debated issue is the storage of such events. Two main options are envisaged: local data storage within individuals' devices, or centralised

storage. The EDPB is of the opinion that both can be valid alternatives, provided that adequate security measures are in place, and that different entities may also be considered as controllers depending on the ultimate objective of the app (e.g. the controller and data processed may be different if the objective is to provide in-app information or to contact the person on the phone, for instance). In any case, the EDPB wants to underline that the decentralised solution is more in line with the minimisation principle.

Finally, these apps are not social platforms for spreading social alarm or giving rise to any sort of stigmatisation. In fact, they should be tools for empowering people to do their part. Quoting the draft Guidance, their sole objective is “*for public health authorities to identify the persons that have been in contact with a person infected by COVID-19 and ask him/her to self-quarantine, rapidly test them, as well as to provide advice on next steps, if relevant, including what to do if developing symptoms*”. The quality of the processed data is of paramount importance in this effort. The steps that need to be taken “*to identify the persons that have been in contact with a person infected by COVID-19*” are not easy or straightforward. Informing a person, via an in-app notification, may be done in such a way that the application processes only random pseudonyms. In addition, a mechanism should ensure that whenever a person is declared as COVID-positive, the information entered in the app is correct, since this may trigger notifications to other people concerning the fact that they have been exposed. Such mechanism could be based, for instance, on a one-time code that can be scanned by the person when the result of a test is given to him/her. Every individual contact must be performed only by health authorities after assessing strong data evidence, with the least amount of inference. In addition, the role of the “*contact list of the person owning the device*”, as envisaged in the Guidance, should be clarified by the Commission.

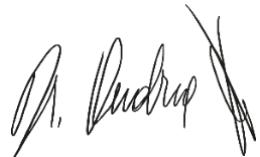
Algorithms used in contact tracing apps should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives, and by no means the task “*to provide advice on next steps*” should be fully automated. It is advisable that a call-back mechanism is put in place where the person is given a telephone number or a contact channel to get more information from a human agent. Also, in order to avoid stigmatisation, no potential identifying element of any other data subject should be part of this “*advice*”, nor should the use of the app, or part of it (like dashboards, configuration settings etc.), allow the re-identification of any other persons, infected by COVID-19 or not. The EDPB strongly suggests not to store any directly identifying data in users’ device and that such data be in any case deleted as soon as possible.

The EDPB strongly supports the concept in the Recommendations that once this crisis is over, such emergency system should not remain in use, and as a general rule, the collected data should be erased or anonymised.

Finally, the EDPB and its Members, in charge of advising and ensuring the correct application of the GDPR and the e-Privacy Directive, should be fully involved in the whole process of elaboration and implementation of these measures. The EDPB recalls that it intends to publish Guidelines in the upcoming days on geolocation and other tracing tools in the context of the COVID-19 out-break.

In all circumstances, the EDPB remains available to provide further guidance to the EU institutions and to all stakeholders involved in the development and use of those mobile apps for the fight against COVID-19.

Yours sincerely,



Andrea Jelinek

Juan Fernando López Aguilar
Chairman of the LIBE Committee, European Parliament

13 November 2019

By email only

Ref: OUT2019-0049

Subject: Your request to the EDPB for a legal assessment on the Commission proposals for Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyyxxx {ECRIS-TCN] - 2019/0001(COD) - COM(2019)0003; and Regulation of the European Parliament and of the Council establishing the conditions/or accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861 - 2019/0002(COD) - COM(2019)0004

Dear Mr López Aguilar,

we would like to thank you for the LIBE Committee's request of 4 April 2019, by which the EDPB was asked for a legal assessment on the implications of the aforementioned Commission proposals on the right to the protection of personal data in the framework of the envisaged automated processing.

The recent Commission proposals have to be seen as part of a bigger picture. At a first glance, they seem to contain only necessary follow-up amendments to Regulation (EU) 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS Regulation)¹. Those amendments concern the ETIAS Regulation itself as well as the legal bases for four other European information systems, namely the Schengen Information System (SIS), the Visa Information System (VIS), the Entry Exit System (EES)² and the European Criminal Record Information System on Third Country Nationals

¹ Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, see <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2018:236:FULL&from=EN>.

² REGULATION (EU) 2017/2226 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, see <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:327:FULL&from=EN>.

(ECRIS-TCN)³. Three of those systems are not yet established. Nevertheless the establishing legislation is already being amended in these Commission proposals.

The EDPB wishes to stress that such a regulatory approach – amending provisions for databases that are not yet in place – does neither align with the principle of transparency nor with the principle that data processing has to be based on clear, precise and accessible rules.

It is necessary to look at this from a holistic point of view where the core items of these proposals should be considered as implementing parts of the new Interoperability Framework⁴. The ETIAS is one of six systems (the five systems already mentioned and Eurodac) that are going to be incorporated in the Interoperability Framework, interconnected by a common search portal, a common identity repository, a common biometric matching service and a common tool for multiple identity detection. The setting up of a common repository for identity data from the EES and the ETIAS will serve as technical basis for the future Common Identity Repository of the Interoperability Framework. The setting up of an instrument for the automated comparisons made by the ETIAS central system in SIS, VIS, EES and ECRIS-TCN will serve as the technical basis for the future European Search Portal (ESP) in the Interoperability Framework. Furthermore, the widened access rights to VIS for law enforcement authorities for identification purposes that are part of the Interoperability Framework marks the final discard of the thresholds put up by Council Decision (EU) 2008/633⁵ for law enforcement agencies' access to VIS.

The Interoperability Framework poses enormous risks to the rights for privacy and data protection. By interconnecting IT systems enabling cross access processes that are difficult to account for the legislator is disregarding its own encoded principle of Data Protection by Design and by Default. The EDPB wishes to recall that the European data protection authorities have already analyzed the implications of the Interoperability Framework and commented on them in detail in the former Working Party 29's Opinion on Commission proposals on establishing a framework for interoperability

³ Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, see <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:135:FULL&from=EN>.

⁴ Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, see <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:135:FULL&from=EN>, and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, see <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:135:FULL&from=EN>.

⁵ COUNCIL DECISION 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, see <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0633&from=EN>.

between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration (WP 266) adopted on 11 April 2018⁶.

The concerns expressed by the WP 29 are still valid. Thus, the recent proposals are only one further step in the big project once tabled in the Communication from the Commission to the European Parliament and the Council “Stronger and Smarter Information Systems for Borders and Security”⁷. Since then there has been a steady flow of new regulatory initiatives with the purpose of extending existing information systems, establishing new information systems and incorporating all of them into the Interoperability Framework that was finally adopted in May 2019 and came into force shortly thereafter.

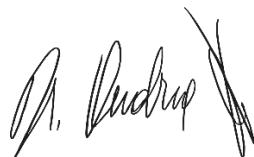
The new architecture for information systems in the field of border management, asylum, migration, police and judicial cooperation has been negotiated with tremendous speed and with a continuous flow of complex legislative proposals, all interconnected with one another. This way of processing has been a clear challenge for the data protection assessments requested. Since the underlying legislation that is the cause for the amendments in these proposals is already in force, the EDPB can only recall all its previously expressed concerns.

The EDPB wishes to express its deep concern with regards to the challenges the Interoperability Framework poses for compliance with the principle of purpose limitation, data subjects’ rights and additionally the fulfillment of supervisory tasks of the data protection authorities.

We remain at your disposal for any questions or clarifications you may require on these subjects.

Yours sincerely,

For the EDPB



Andrea Jelinek

⁶ see https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624198

⁷ COM (2016) 205 final, see <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52016DC0205>.

Opinion of the Board (Art. 64)



Opinion 16/2019 on the draft decision of the Belgian Supervisory Authority regarding the Binding Corporate Rules of ExxonMobil Corporation

Adopted on 12 November 2019

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	4
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 (EEA) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018, as last amended on 10 September 2019,

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 European Economic Area. To this effect, it follows from article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (SA) aims to approve binding corporate rules (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 the 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, in addition, conferred to the EDPB the task to issue an opinion on the competent supervisory authority’s (BCR Lead) draft decision aiming to approve BCRs. This task of EDPB aims to ensure the consistent application of the GDPR, including by the supervisory authorities, controllers and processors.
- (3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. 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 supervisory authority (“competent SA”), in accordance with the consistency mechanism set out in article 63 and 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 Party¹, endorsed by the EDPB.

(4) WP256 rev.01 of the Article 29 Working Party,² as endorsed by the EDPB, provides for the required elements for BCRs for controllers, 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 to the supervisory authorities' national laws. The EDPB is subject to Regulation 1049/2001 pursuant to article 76(2) GDPR.

(5) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2), each application should be addressed individually and is without prejudice to the assessment of any other Binding Corporate Rules. 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.³

(6) 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 Controller BCRs of ExxonMobil Corporation were reviewed by the Belgian Data Protection Authority (hereinafter Belgian Supervisory Authority) as the BCRs Lead SA.
2. The Belgian Supervisory Authority has submitted its draft decision regarding the draft Controller BCRs of ExxonMobil Corporation, requesting an opinion of the EDPB pursuant to article 64(1)(f) GDPR on 15/10/2019. The decision on the completeness of the file was taken on 16/10/2019.

2 ASSESSMENT

3. The ExxonMobil Corporation draft Controller BCRs apply to processing, within the group, of personal data that are governed by the GDPR or were governed by the GDPR prior to transfer to a group member outside the EEA. The ExxonMobil Corporation draft Controller BCRs cover the transfer of

¹ 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.

² 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.

³ 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.

aforementioned personal data to any of the group members globally as well as their subsequent processing by group members. The ExxonMobil Corporation draft Controller BCRs are integrated within an overarching global data protection policy which applies to processing of any personal data within the group regardless of origin. Concerned data subjects include current and past employees, job applicants, contractors, representatives of customers and other business partners, and consumers.

4. The ExxonMobil Corporation draft Controller BCRs have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the ExxonMobil Corporation draft Controller BCRs contain all elements required under article 47 GDPR and WP256 rev01, in concordance with the draft decision of the Belgian Supervisory Authority submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns which need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

5. Taking into account the above and the commitments that the group members will undertake by signing ExxonMobil Corporation's Intra-Group Agreement on Binding Corporate Rules, the EDPB considers that the draft decision of the Belgian Supervisory Authority may be adopted as it is, since those Rules ensure appropriate safeguards to ensure that the level of protection of natural persons guaranteed by this Regulation 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 WP 256 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

6. This opinion is addressed to the Belgian Supervisory Authority and will be made public pursuant to article 64(5)(b) GDPR.
7. According to Article 64(7) and (8) GDPR, the Belgian Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
8. Pursuant to article 70(1)(y) GDPR, the Belgian Supervisory Authority 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 17/2019 on the UK data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 02 December 2019

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 UK 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	8
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES	9
2.2.6	TRANSPARENT COMPLAINT HANDLING	9
2.2.7	COMMUNICATING WITH THE ICO	10
2.2.8	CODE REVIEW MECHANISMS	10
2.2.9	LEGAL STATUS	11
3	CONCLUSIONS / RECOMMENDATIONS	11
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 2018,¹

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 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, to provide written guidance explaining the accreditation requirements; and, finally, requesting them to adopt these 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

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

their proposed monitoring body meets the requirements set out in article 41 (2) 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 United Kingdom Supervisory Authority (hereinafter "UK 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 4th September 2019.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the initial adoption period of eight weeks was extended 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 UK SA to take further action.
8. The Board notes that the document submitted by UK SA contains not only the accreditation requirements, but also explanatory notes, which include general and specific explanations about the UK SA’s approach to accreditation requirements.
9. This opinion does not reflect upon items submitted by the UK 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 UK accreditation requirements for Code of Conduct’s monitoring bodies

10. 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

11. The Board observes that the introduction section for the UK SA’s accreditation requirements refers to both the Guidelines and the Opinion 9/2019 on the Austrian SA’s draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR. Whereas the reference to the Guidelines is welcomed, the Board encourages the UK SA to delete the reference to a specific Opinion, and to make a more general statement instead, considering that other opinions of the Board will follow

in relation to the accreditation requirements submitted by other SAs. An example could be: “This document should be read alongside the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 and the relevant Opinions of the EDPB pursuant to articles 41 (3) and 64 (1) (c)GDPR”.

12. With regard to the “general notes”, the Board is of the opinion that the references to the legal bases in the second paragraph should also include article 57 (1) (p) GDPR. The Board encourages the UK SA to amend the “general notes” section accordingly.
13. The Board notes that, in the section “accreditation requirements”, the UK SA does not make any reference to the language in which the documents must be submitted. The Board encourages the UK SA to clarify in the accreditation requirements the language or languages accepted.
14. The Board observes that, in the section “accreditation requirements”, the UK SA establishes the validity of the accreditation to five years, after which a review of the accreditation will be carried out. The Board notes that article 41 GDPR does not refer to the validity of the accreditation of a monitoring body, and understands that there is 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. However, for the sake of clarity, the Board encourages the UK SA to provide transparent information on what happens after the expiry of the validity of the accreditation and what the procedure will be.
15. The Board notes that, for some accreditation requirements, it is not clear whether a specific requirement applies to all monitoring bodies, regardless of their nature (internal or external monitoring body), or to a specific kind of monitoring bodies. The Board is of the opinion that the UK SA should specify, for instance, in the “general notes” section at the beginning of the document, that the requirements listed in the document shall apply to the monitoring body, regardless of whether it is internal or external. Moreover, if the UK SA intends to set out a requirement specifically for an internal or external monitoring body (see for example subsection 1.3.1 of the draft accreditation requirements which refers only to an internal monitoring body), it should be specified clearly in the document to avoid confusion. Therefore, the Board recommends the UK SA to amend the draft accordingly.
16. The Board observes that the UK SA’s accreditation requirements sometimes refer to an obligation (“shall”) and sometimes to a possibility (“should”). For the sake of clarity, the Board recommends that the UK SA avoids the use of “should” in the text of the accreditation requirements. With regard to the explanatory notes, the Board encourages the UK SA to replace “should” with “will”. On a similar note, the Board notes that the UK SA’s accreditation requirements sometimes refer to “staff” and sometimes to “personnel”. If the distinction entails any difference, the Board encourages the UK SA to make it clear.

2.2.2 INDEPENDENCE

17. With regard to the explanatory note on the independence of the monitoring body (section 1), the Board notes that the second paragraph provides that (underline added) “*internal bodies may be required to provide evidence [...]*”. However, in section 1.1 (Legal and decision-making procedures) the UK SA uses the word “shall”. The Board encourages the UK SA to adapt the wording of the explanatory note to be in line with paragraph 16 above.

18. With regard to section 1.1 (Legal and decision-making procedures), the Board welcomes the approach taken in subsection 1.1.2 of the draft accreditation requirements, providing examples of the means by which evidence of the monitoring body's independence can be produced. The Board considers, nonetheless, that the example referring to "*powers and operation of any committees that may be involved with an internal monitoring body*" would be more comprehensive if it included a general reference to the personnel who are in charge of the decision-making of the monitoring body. The Board notes that a monitoring body does not necessarily need to be organised in committees, since individuals can also be in charge of making decisions. Therefore, the Board encourages the UK SA to amend the example taking into account that individuals could also be in charge of the decision-making.
19. With regard to the evidence of the independence of the monitoring body personnel (subsection 1.1.3), the Board encourages the UK SA to follow the same approach taken in the previous subsection and provide examples as to how the monitoring body can provide such evidence.
20. As for the financial requirements (section 1.2), the Board considers that they 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 (subsection 1.2.3). 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 UK SA to provide examples of how the monitoring body can provide such evidence.
21. The Board notes that subsection 1.3.2 of the UK SA accreditation requirements contains an example of how the monitoring body can demonstrate organisational independence "*by using different logos or names where appropriate*". The Board welcomes the introduction of examples that facilitate the practical application of the requirements. However, the Board considers that, in this particular case, the example given is more relevant for internal monitoring bodies. As a result, the Board encourages the UK SA to clarify if that is the case and, if so, to specify that in the example.
22. The Board encourages the UK SA to develop subsection 1.3.3 in more detail, in order to provide a better understanding of the criteria to consider that resources and staffing are sufficient for the monitoring body to effectively perform its tasks. In this regard, 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 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, contract or other formal agreement with the monitoring body.
23. With regard to the accountability requirements (section 1.4), the Board considers that the UK SA should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate its accountability. The Board welcomes the general reference to the accountability requirement in subsection 1.4.1, but there is a need to specify its content, defining the approach that the UK SA will take in this regard, and how the compliance with the requirement will be assessed. This could be done, for instance, by setting up policies to increase awareness among the staff about the governance

structures and the procedures in place (e.g. training). Thus, the Board recommends the UK SA to clarify the requirements for accountability, to allow for a better understanding of its content and offer more examples of the kind of evidence that the monitoring bodies can provide.

24. In subsection 1.4.2 of the UK SA accreditation requirements is not clear as to whether the term “any other organisation” includes also the code owner. Moreover, the Board notes that the wording could be rephrased in order to better reflect that the monitoring body shall make any kind of decision freely. Therefore, the Board encourages the UK SA to rephrase subsection 1.4.2 in order to mirror this. A drafting example could be: “Any decisions made by the monitoring body related to its functions shall not be subject to approval by any other organisation, including the codes owner”.

2.2.3 CONFLICT OF INTEREST

25. Section 2.2 of the UK SA accreditation requirements include a reference to staff “*provided by a body independent from the code*”. The Board acknowledges that this wording is taken from the Guidelines and welcomes its inclusion in the UK SA accreditation requirements. Nonetheless, the Board is of the opinion that, from a practical point of view, some examples might also be helpful. An example of staff provided by a body independent of the code would be monitoring body personnel that have been recruited by an independent external company, which provides recruitment and human resources services. Therefore, the Board encourages the UK SA to add an example in line with the one provided in this paragraph.

2.2.4 EXPERTISE

26. The Board notes that the UK SA’s expertise requirements include: an in-depth understanding, knowledge and experience in relation to the specific data processing activities in relation to the code (section 3.1 of the UK SA’s accreditation requirements), appropriate data protection expertise and operational experience (section 3.2) and, finally, the necessary expertise requirements as defined in the code of conduct (section 3.3).
27. The Board further acknowledges that the guidelines set a high bar requiring monitoring bodies to have the following expertise: an in-depth understanding of data protection issues, knowledge of the specific processing activities in relation to the code and appropriate operational experience and training for monitoring, such as auditing.
28. The Board considers that the accreditation requirements need to be transparent. They also need to provide for monitoring bodies seeking accreditation in relation to codes that cover micro, small and medium-sized enterprises’ processing activities (article 40 (1) GDPR).
29. As required by the Guidelines, every code must fulfil the monitoring mechanism criteria (in section 6.4 of the Guidelines), by demonstrating ‘why their proposals for monitoring are appropriate and operationally feasible’ (paragraph 41, page 17 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. To that end, in order to evaluate the expertise level required by the monitoring body, it should, in general, be taken into account such factors as: the size of the sector concerned, the different interests involved and the risks of the processing activities addressed by the code. This would also be important if there are several monitoring bodies, as the code will help ensure a uniform application of the expertise requirements for all monitoring bodies covering the same code.

30. In this regard, the Board considers that section 3.3 of the UK SA's accreditation requirements referring to the "*necessary expertise requirements [...] defined in the code of conduct*" should be better coordinated with section 3.1 and section 3.2, in order to avoid confusion with regard to the scope of section 3.3 in connection with the previous two. Therefore, the Board encourages the UK SA to clarify the relationship between those sections specifying that the monitoring body will have to meet the expertise requirements in sections 3.1 and 3.2 in any circumstances, whereas further or specific expertise requirements will only need to be met in case that the code of conduct foresees them.
31. The expertise of each monitoring body should be assessed in line with the particular code. Whereby the SA will verify if the monitoring body possesses adequate competencies for the specific duties and responsibilities to undertake the effective monitoring of the code. The Board encourages the UK SA to ensure that the reference to appropriate data protection expertise, included in section 3.2, is related to the specific sector of the code.
32. The Board observes that the UK SA's expertise requirements refer to the "relevant personnel" of the monitoring body in section 3.2, without further clarifying the concept and what are the criteria to consider the personnel relevant. The Board recommends the UK SA to further clarify the notion of "relevant personnel", explaining how the relevant personnel has to be identified. The clarification could be included in the explanatory notes for this section, providing some practical examples, e.g. personnel conducting audits or making decisions on behalf of the monitoring body.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

33. The explanatory note for section 4 of the UK SA accreditation requirements establishes that "*the monitoring body shall apply the penalties as defined in the code of conduct*". By only referring to penalties, the explanatory note seems to restrict the margin of manoeuvre of the monitoring body with regard to the kind of measures it can apply. The Board considers that a more comprehensive wording would also mention corrective measures, and encourages the UK SA to add the suggested reference in the explanatory note.

2.2.6 TRANSPARENT COMPLAINT HANDLING

34. With regard to the complaints handling procedure, the Board observes that the explanatory note states that "*personnel should demonstrate sufficient knowledge and impartiality*". The Board considers that the level of knowledge required to handle complaints would be better understood if the UK SA refers to "adequate knowledge" defining its meaning and therefore it encourages the UK SA to do so.
35. Regarding the complaints about code members (section 5.1 of the UK SA accreditation requirements), the Board acknowledges that complaints handling process requirements should be set at a high level and reference reasonable time frames for answering complaints. In this regard, the Board notes that the UK SA accreditation requirements state that the monitoring body shall provide the complainant with progress reports and the outcome of the complaint within three months. In the event that, by the term "outcome", the UK SA refers to the final decision in the investigation, the Board recommends the UK 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. If the UK SA refers to another kind of outcome, different from the final decision of the investigation, the Board recommends the UK SA to clarify what kind of information it is referring to.
36. Furthermore, the Board considers that the three months deadline could be extended where appropriate (e.g. taking into account the size of the company under investigation). The Board therefore

encourages the UK SA to include this possibility in this section's explanatory note or in the requirements.

37. The Board notes that, in subsection 5.1.3, the UK SA's accreditation requirements refer to corrective measures, such as "*training, issuing a warning, report to the board of the member, formal notice requiring action, suspension or exclusion from the code*". Those corrective measures must be determined in the code of conduct, as per article 40(4) GDPR. Therefore, for the sake of clarity, the Board recommends the UK 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.
38. The Board observes that the accreditation requirements entail that the monitoring body publishes information about the decisions taken in the context of the complaint handling procedure (subsection 5.1.6). Publication of final decisions could have the same effect of an accessory sanction for the code member to which the decision is addressed. However, general information on the complaints handled by the monitoring body would benefit from transparency. For example, the monitoring body could publish, on a regular basis, statistical data with the result of the monitoring activities, such as the number of complaints received, the type of infringements and the corrective measures issued. Thus, for the sake of clarity, the Board recommends that the UK SA specifies the kind of information that the monitoring body is obliged to publish.

2.2.7 COMMUNICATING WITH THE ICO

39. With regard to the communication of substantial changes to the UK SA (referred to in the accreditation requirements as the ICO), the Board notes that the accreditation requirements state that substantial changes "*could result in a review of the accreditation*" (section 6.4 and explanatory note). The Board is of the opinion that, when a substantial change has been performed, the review of the accreditation is not merely a possibility, but rather an obligation. Therefore, the Board recommends the UK SA to rephrase the wording, by stating that substantial changes would result in a review of the accreditation.
40. The Board recommends that the obligation for the monitoring body to report to the competent SA, without undue delay, any substantial change, is explicitly outlined in the accreditation requirements.

2.2.8 CODE REVIEW MECHANISMS

41. The Board observes that the UK SA's accreditation requirements provide that the monitoring body shall set up plans and procedure aiming at ensuring "*that the code remains relevant to the members and continues to meet the application of the GDPR*" (section 7.1). The Board notes that it is the role of the code owner to ensure the continued relevance and compliance of the code of conduct with applicable legislation. The monitoring body is not responsible to carry out that task, but it shall contribute to any review of the code. As a result, the Board recommends the UK SA to provide accreditation requirements that make clear that the monitoring body will contribute to any review of the code.
42. The accreditation requirements contain an obligation to provide the code owner with an annual report on the operation of the code (section 7.3). The Board considers that this requirement should envisage the possibility that the annual report is provided not only to the code owner, but also to any other entity referred to in the code of conduct, in order to give some margin of manoeuvre to the code owners in designing the procedure for assessing the necessity of a revision of the code. The Board therefore encourages the UK SA to take this into consideration and add the above-mentioned reference.

43. The Board is of the opinion that more information on the content of the report should be included in the accreditation requirements. An example would be an audit report that includes the date of the audit, its scope, the identity of the auditee, the audit conclusion, if corrective measures are applicable, if a complaint received against the auditee, etc. The Board encourages the UK SA to add more details with regard to the kind of information that the monitoring body is expected to include in the annual report.
44. In addition, the Board considers that the monitoring body should compile all the information related to the audits carried on, and have that information at the disposal of the UK SA. Therefore, the Board encourages the UK SA to take this into account and add such provision.

2.2.9 LEGAL STATUS

45. With regard to the legal status of the monitoring body, the UK SA's explanatory note for this section states that the monitoring body "*must demonstrate sufficient financial and other resources to deliver its specific duties and responsibilities*". The Board considers that the existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time. Thereby, the Board encourages that the UK SA amend the explanatory note, adding the above-mentioned reference to "procedures".

3 CONCLUSIONS / RECOMMENDATIONS

46. The draft accreditation requirements of the United Kingdom Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
47. As general remarks, the Board recommends that the UK SA:
 1. specifies at the beginning of the document, or in the "general notes", that the requirements listed in the document shall apply to the monitoring body, regardless of whether it is an internal or external monitoring body, unless otherwise specified.
 2. avoids the use of "should" in the text of the accreditation requirements.
48. Regarding 'independence' the Board recommends that the UK SA:
 1. clarifies the requirements for accountability and offers more examples of the kind of evidence that the monitoring bodies can provide.
49. Regarding 'expertise' the Board recommends that the UK SA:
 1. clarifies the concept of "relevant personnel" by explaining how the relevant personnel will be identified and providing practical examples, for example, personnel conducting audits or making decisions on behalf of the monitoring body.
50. Regarding 'transparent complaint handling' the Board recommends that the UK 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 time, such as three months. If the UK SA refers to another kind of outcome, different from the final decision of the investigation, the Board recommends that the UK SA should clarify what kind of information it is referring to.

2. adds a reference to the list of sanctions as set out in the code of conduct.
 3. clarifies the kind of information that the monitoring body is obliged to publish.
51. Regarding 'communication with the ICO (UK SA)' the Board recommends that the UK SA:
1. states that the substantial changes would result in a review of the accreditation
 2. adds the obligation to report to the competent SA, without undue delay, any substantial change.
52. Regarding 'code review mechanisms' the Board recommends that the UK SA:
1. makes clear that the monitoring body will contribute to any review of the code.

4 FINAL REMARKS

53. This opinion is addressed to the United Kingdom supervisory authority and will be made public pursuant to Article 64 (5)(b) GDPR.
54. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft 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 supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

EU - U.S. Privacy Shield - Third Annual Joint Review

Adopted on 12 November 2019

Table of contents

1	Executive summary	4
1.1	Introduction.....	4
1.2	On the commercial aspects of the Privacy Shield	4
1.3	On the access by public authorities to data transferred to the U.S. under the Privacy Shield	5
1.4	Conclusion	7
2	Introduction.....	9
3	On the commercial aspects of the Privacy Shield	10
3.1	Guidance for the companies adhering to the Privacy Shield	10
3.2	Clear and easily available information for EU individuals	11
3.3	Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism	11
3.4	Oversight and supervision of compliance with the Principles – Activities of the DoC.....	13
3.5	Oversight and supervision of compliance with the Principles – Activities of the FTC	14
3.6	Independent Recourse Mechanisms	15
3.7	HR Data.....	15
3.8	Automated-decision making/Profiling	16
4	On the derogations to the Privacy Shield to allow access to data for Law Enforcement and National Security purposes	17
4.1	Introduction.....	17
4.2	Collection of data (under section 702 and under EO 12333).....	17
4.2.1	Collection of data for national security purposes under Section 702.....	17
4.2.2	Collection of data for national security purposes under Executive Order 12333.....	18
4.2.3	Safeguards provided in Presidential Policy Directive 28 (PPD-28)	18
4.3	Oversight	19
4.4	Redress for EU individuals.....	20
4.5	Ombudsperson mechanism	20
4.6	Access to data for law enforcement purposes.....	22
5	Conclusion	22
ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW ...		24
General Information.....		24
1	On commercial aspects	24
1.1	Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program.....	24
1.2	Oversight and supervision of compliance with the principles - Activities by the DoC.....	25
1.3	Independent Recourse Mechanism (IRM).....	27

1.4	Arbitral Panel.....	27
1.5	Oversight and supervision of compliance with the principles - Activities by the FTC.....	27
1.5.1	Concerning the status of the Privacy Shield enforcement in general.....	27
1.5.2	On the Facebook case which led to the recent settlement with the FTC (follow-up of the discussions in the second Joint Review and update on this case)	28
1.5.3	On the general developments in US privacy law that may affect the Privacy Shield and on the resources of the FTC	28
1.6	Oversight and supervision of compliance with the principles - Activities by the DoT.....	29
1.7	Onward Transfers.....	29
1.8	Automated decision-making/Profiling	30
1.9	HR Data.....	30
1.10	US domestic privacy update: NIST Framework	30
2	On government access to personal data: relevant developments in the U.S. legal framework and trends	30
2.1	Ombudsperson mechanism	30
2.2	Inspector General (IG)	31
2.3	PCLOB	31
2.4	ODNI and Department of Justice presentation and Q/A on government access to personal data: relevant developments in the U.S. legal framework and trends	32
	List of abbreviations	34

The European Data Protection Board

Having regard to Article 4 and Recitals 145 to 149 of the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (“EU - U.S. Privacy Shield),

HAS ADOPTED THE FOLLOWING REPORT:

1 EXECUTIVE SUMMARY

1.1 Introduction

1. According to the EU-U.S. Privacy Shield adequacy decision (“Privacy Shield”)¹ adopted on 12 July 2016, **eight representatives of the EDPB participated in the third joint review conducted by the European Commission, on September 12 and 13 of 2019** in Washington to assess the robustness of its adequacy decision and its practical implementation.
2. Based on the concerns elaborated in the previous opinions of the WP29 and of the EDPB, in particular opinion 1/2016, and the reports following the first and second joint review, the EDPB focused on the assessment of both the **commercial aspects** of the Privacy Shield and on the **government access to personal data transferred from the EU for the purposes of Law Enforcement and National Security, including the legal remedies available to EU individuals**.² The EDPB assessed once again whether these concerns have been addressed and also whether the safeguards provided under the EU-U.S. Privacy Shield are workable and effective.
3. The European Commission published its report of the third joint review on October 23, 2019.
4. **The EDPB’s main findings concerning this third joint annual review**, stemming both from written submissions and from oral contributions are hereby presented in this report.

1.2 On the commercial aspects of the Privacy Shield

5. The third annual review showed that the U.S. authorities have continued their efforts to implement the Privacy Shield.
6. **The DoC as well as the FTC also undertook new ex officio oversight and enforcement actions as regards the compliance of Privacy Shield certified organizations** with the requirements under the Privacy Shield. The EDPB particularly welcomes that the DoC has increased the number of “random spot checks” to 30 organizations per month.
7. **However, one of the main concerns already expressed by the WP29 and the EDPB remains a certain lack of oversight in substance.** Indeed, the checks performed by the DoC are principally focused on formal aspects. The enforcement actions by the FTC focused on procedural violations of the framework

¹ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.

² Any reference to the “EU” shall be understood as a reference to the “EEA”, in accordance with Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 and Decision of the EEA Joint Committee No 144/2017 of 7 July 2017.

rather than on the substance. This lack of substantial checks thus remains a concern of the EDPB as, even taking into account discretionary and limited investigations by the FTC, a majority of companies' compliance with the substance of the Privacy Shield's principles remains unchecked, although many of them were introduced or further detailed compared to the Safe Harbor. In addition, the increase of complaints, in general, although resolved successfully, does not entirely compensate for this lack of proactive checks on substance. Indeed, these complaints do not seem to concern the issues of concerns underlined by the EDPB so far as they seem to mainly focus on procedural aspects.

8. **One example for which the EDPB sees the need for more substantive checks are onward transfers.** Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance that the competent US Authorities closely monitor the practical implementation of the Privacy Shield's "Accountability for the Onward Transfers Principle". As a first step, for example the DoC could make use of its right to ask organizations to produce the contracts they have put in place with third countries' partners in order to assess whether those provide the necessary safeguards and to discover if any further guidance or other action by the DoC or the FTC is needed.
 9. **Another area that requires further attention is the application of the Privacy Shield requirements regarding HR Data.** While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the European Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations lead to gaps in the protection of EU data subjects.
 10. **Also, the re-certification process needs to be further refined.** The situation of outdated listings leads to avoidable confusion that should be addressed also in the interest of concerned Privacy Shield certified organizations.
 11. Last but not least, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016 in particular regarding the absence or the limitation to the rights of the data subjects (i.e. right to object, right to access, right to be informed for HR processing), the absence of key definitions, the application of the principles when it comes to "processors", the lack of guarantees on transfers for regulatory purpose in the field of medical context, the lack of specific rules on automated decision making and the overly broad exemption for publicly available information. Those remain valid.
- 1.3 [On the access by public authorities to data transferred to the U.S. under the Privacy Shield](#)
12. The EDPB **welcomes the appointments of the last missing members of the Privacy and Civil Liberties Oversight Board (PCLOB)**, enabling it to be fully functioning and operational, as well as its increased transparency concerning its work plan.
 13. **The EDPB also welcomes the appointment of Mr Keith Krach, as "permanent" Ombudsperson on 18 January 2019.**
 14. Despite these developments, **some of the main points of concern, already expressed by the WP29 and the EDPB in this area in their previous reports, still have to be fully resolved.**

15. More specifically, the **collection and access of personal data for national security purposes** under both Section 702 of FISA³ and Executive Order 12 333⁴ still remains an important issue for the EDPB.
16. In this respect, the EDPB recalls that it continues to consider that within the surveillance programs, more specific safeguards would be needed, e.g. for precise targeting to determine whether an individual or a group can be a target of surveillance and for stricter scrutiny of individual targets by an independent authority ex-ante.
17. In addition, although it acknowledges the efforts that the PCLOB has undertaken to follow-up on its past recommendations concerning section 702 FISA, as well as to issue a new report on the FBI's querying of data under Section 702, **the EDPB deeply regrets that the PCLOB will not issue further reports** on PPD-28⁵ to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, as well as a general updated report on Section 702 FISA, especially since it was reauthorized with few adjustments since the last Joint Review. The EDPB indeed recalls, as the WP29 did before, that reports of the PCLOB were very useful to feed the assessment led by the WP29 and by the EDPB and would in particular be useful to assess whether the collection of data under Section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program, and for assessing the necessity and proportionality of the definition of "targets", the tasking of selectors under **Section 702** (including in the context of the **UPSTREAM program**⁶), as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive access to data occurs in this context. Concerning the application of **Executive Order 12 333** to EU data transferred to the U.S., the EDPB will welcome the finalization by PCLOB of its awaited reports on EO 12 333. However, as the EDPB understands that these reports will most likely remain classified, they may not be used as a relevant source of information on the concrete operation of this Executive Order and on its necessity and proportionality.
18. Access to such reports **would allow the EDPB to provide a comprehensive assessment of these aspects**. It consequently stresses that, in order to perform more meaningful reviews, it could benefit from accessing to additional documents and discussing additional classified elements, following the examples of PNR or TFTP reviews.

³ See the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 et seq.) (FISA) – its section 702 allows for data to be collected from non-U.S. persons reasonably believed to be outside the United States in order to obtain foreign intelligence information (50 U.S. Code §1881a (D)(1))

⁴ See footnote 59 of the Privacy Shield Adequacy Decision: “E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 December 1981). To the extent that the Executive Order is publicly accessible, it defines the goals, directions, duties and responsibilities of U.S. intelligence efforts (including the role of the various Intelligence Community elements) and sets out the general parameters for the conduct of intelligence activities (in particular the need to promulgate specific procedural rules). According to Sec. 3.2 of E.O. 12333, the President, supported by the National Security Council, and the DNI shall issue such appropriate directives, procedures and guidance as are necessary to implement the order.”

⁵ “PPD-28 is a directive of the President of the United States laying down consistency principles with which signals intelligence collection shall be authorised and conducted but PPD-28 is not a legal basis for collection” – See [Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision](#) of the WP 29 as well as annex VI of the Privacy Shield Decision

⁶ See [WP29 report on the Privacy Shield of 28 November 2017](#) (page 15): “Two programs are confirmed to be operating under Section 702 of FISA: PRISM and UPSTREAM. (...)Under PRISM, the relevant U.S. authorities require internet service providers to provide them with the data of their users corresponding to “selectors”, once “tasked” by the competent authority.

Under the UPSTREAM program, the providers of the telecommunication backbone are required to assist the NSA by identifying and collecting transiting data “to” and “from” a chosen “selector” in the flow of communications between communication service providers.”

19. Due in particular to the problematic admissibility threshold of the “**standing requirement**”, the redress by EU citizens before U.S. courts is still to be effectively guaranteed. Therefore, the EDPB will continue to follow closely the evolution of the case law.
20. Hence, the independence of the Ombudsperson remains a key element, as this institution is designed to compensate the uncertainty in seeking effective redress before the court, if not the lack thereof.
21. During the third annual review, it was clarified that any violation of the targeting and minimisation procedures under Section 702 FISA would be reported to the FISC by the Ombudsperson, in which case the FISC may decide to issue a deficiency order. Despite further discussions on the procedural aspects of the (inadmissible) first case referred to the Ombudsperson by the EU Centralized Body earlier this year, as well as on hypothetical cases which brought some clarifications, the exact powers of the Ombudsperson still need to be clarified, through the **declassification of internal procedures** concerning the interactions between the Ombudsperson and the other elements of the intelligence community or oversight bodies. Based on the information provided so far, the EDPB is of the view that the Ombudsperson’s access to information, which appears to remain indirect, and its powers to remedy non-compliance vis-à-vis the intelligence authorities, are still not sufficient in the light of Article 47 EU Charter of Fundamental Rights. It also underlines that the Ombudsperson is not in a position to bring a matter before the court other than to bring a violation of Section 702 FISA to the attention of the FISC.
22. Finally, regarding the **access to data for law enforcement purposes**, the EDPB underlines its remaining concerns on the available effective remedies for individuals in cases where the personal data processed by companies are accessed by law enforcement authorities.

1.4 Conclusion

23. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially ex officio oversight and enforcement actions, as well as the appointments of the last missing members of the PCLOB and of a permanent Ombudsperson.**
24. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities.**
25. As regards the **commercial aspects, the absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR data and the application of the principles when it comes to processors, as well as the recertification process. More generally, the members of the Review Team would benefit from a broader access to non-public information, concerning commercial aspects and ongoing investigations.** In addition, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29’s Opinion 01/2016.
26. As regards the **collection of data by public authorities, the EDPB can only encourage the PCLOB to issue and publish further reports. It regrets that on Section 702 FISA no general report is contemplated, to provide an assessment of the changes brought since the last reauthorization in 2018. The EDPB would be very interested on an additional report on PPD-28 to follow up on the first report** including an assessment of how the safeguards of PPD-28 are applied. Finally, the EDPB underlines the importance of reports on Executive Order 12 333, and regrets that those reports will most likely remain classified. In this regard, the EDPB stresses that the members of the review team only have access to the same documents as the general public. **The EDPB recalls that the security cleared experts of the**

EDPB remain ready to review additional documents and discuss additional classified elements, in order to have more meaningful reviews, following the example of PNRs or TFTP reviews.

27. **On the Ombudsperson mechanism**, despite some new elements provided during this year's review, especially on the procedural aspects in relation to the first case submitted to the Ombudsperson but declared inadmissible, as well as on hypothetical cases, **the EDPB is still not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Thus, it still cannot state that the Ombudsperson can be considered an “effective remedy before a tribunal” in the meaning of Art. 47 of the EU Charter of Fundamental Rights.**
28. Finally, the EDPB recalls that the **same concerns will be addressed by the Court of Justice of the European Union in cases that are still pending before it.**

2 INTRODUCTION

29. On 6 October 2015⁷, the European Court of Justice invalidated the Safe Harbor adequacy decision after having recalled the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection. Soon after, the Commission started negotiations for a new adequacy decision and presented a draft adequacy decision with its annexes.
30. On the 13 April 2016, the Working Party 29 issued an opinion⁸ on the draft new adequacy decision aiming at replacing the invalidated Safe Harbor. On the same day, the WP29 also issued a working document⁹ on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).
31. On 30 May 2016, the European Data Protection Supervisor also issued an Opinion on the draft adequacy decision¹⁰.
32. On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield adequacy decision¹¹ ("Privacy Shield"), which has also been incorporated into the EEA Agreement¹². The Privacy Shield entrusts the Commission with the task to assess the findings of the adequacy decision, including on the basis of the factual information collected in the context of an Annual Joint Review¹³. Important concerns on both the commercial aspects and aspects relating to government access to personal data transferred under the Privacy Shield for the purposes of Law Enforcement and National Security had then to be addressed and further assessed in the context of the Joint Review.
33. In addition, it is also foreseen in recital 147 of this adequacy decision that the Commission will meet a number of US authorities, and that the "*participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party*".
34. The WP 29 also issued a report following the first Joint Review of the Privacy Shield in November 2017¹⁴ as well as a second report following the second Joint Review in January 2019¹⁵.
35. The third Joint Review of the Privacy Shield took place on the 12 and 13 September 2019 in Washington D.C. Eight representatives of the EDPB, a Commissioner as well as experts at staff level, were

7 Case C-362/14

8 WP 238 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

9 WP 237 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

10 EDPS Opinion 4/2016 of 30 May 2016: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf

11 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.

12 Decision of the EEA Joint Committee No 144/2017 of 7 July 2017 – Recital (1): "the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (1) is to be incorporated into the EEA Agreement".

13 See recitals 145-149 and Article 4(4) of the decision.

14 WP 255: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

15 EU - U.S. Privacy Shield - Second Annual Joint Review - Adopted on 22 January 2019

designated to be part of the Review Team (“the Review Team”) that accompanied the Commission during this two-day meeting with U.S. authorities, companies’ representatives, NGOs and a representative from the binding arbitration mechanism.

36. In advance to the Joint Review, the Commission sent questionnaires to US trade associations representing Privacy Shield certified organizations and NGOs, as well as a detailed agenda to organize the discussions with the US authorities and stakeholders during the Joint Review itself. The EDPB sent contributions to take part to the elaboration of these documents.
37. Right before the Joint Review, the Commission and the Review Team met with some of the NGOs to further discuss their input on the Privacy Shield.
38. Also, briefly before the actual Joint Review took place in Washington, the EU-Supervisory Authorities representatives were contacted by the DoC to informally discuss the existing divergences on the interpretation of the notion of HR Data (see I. 7.)
39. The new factual elements presented by the US authorities companies’ representatives, NGOs and by a representative from the binding arbitration mechanism participating in the Joint Review, stemming both from written submissions, as well as from oral contributions during the Joint Review itself, are presented in annex to this document. They were presented at the EDPB Plenary on 8 October 2019.

3 ON THE COMMERCIAL ASPECTS OF THE PRIVACY SHIELD

3.1 Guidance for the companies adhering to the Privacy Shield

40. The EU-U.S. Privacy Shield is an adequacy decision that was designed to frame transfers of personal data outside the protections provided under GDPR to ensure the level of protection of natural persons guaranteed by GDPR is not undermined in the absence of a general law in the US providing for an essentially equivalent level of protection of personal data. It is of utmost importance that there is a common understanding of the text to ensure the application in the receiving State will correspond to the requirements for such transfers as set out under EU data protection law. It has to be ensured that this text is interpreted correctly and that organizations and individuals on both sides of the Atlantic are “on the same page” as regards their duties and rights under the Privacy Shield.
41. Thus, in the report of the first annual review the WP 29 emphasized the need for clear guidance on the application of the Privacy Shield principles. In the second year of operation of the framework and following informal consultation of members of the ITS at working level, the DoC has issued **guidance in the form of FAQs on the Accountability for Onward Transfer Principle¹⁶ and the notion of Processor¹⁷** and published it on its website. In the third year of operation of the framework the DoC issued one more guiding document also in the form of FAQs on the Privacy Shield and the UK aiming at issues related to Brexit. The EDPB has not been involved in any way in the drafting of these new FAQs.
42. Since the last joint review, not much additional guidance was published by the US authorities. In this regard, the EDPB recalls in particular that guidance concerning processors may further specify the

¹⁶ <https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs> (last accessed on 18 December 2018)

¹⁷ <https://www.privacyshield.gov/article?id=Processing-FAQs> (last accessed on 18 December 2018)

application of the principles when it comes to processors ("agents").¹⁸ Also, the use of Standard Contractual Clauses as a tool for onward transfers remains to be examined.

43. The EDPB still regards the issuance of guidance as a good start and expects that in the future there will be more guidance as to other key elements. In previous reports, the EDPB already suggested to further work for example the **Choice Principle** (on when and how a data subject can opt out from the processing of his/her data for a new purpose), or on the **application of the Notice Principle** (more specifically on the timing for certified organizations to give notice to individuals). In addition, it recalls that a **clarification of the scope of the right of access** could be helpful to prevent misunderstandings. In its last report, worries regarding the possibly very narrowly interpreted duty to grant the right of access only to data that is "stored" by an organization voiced by the WP 29 still remains valid.

3.2 Clear and easily available information for EU individuals

44. The WP 29 had found that to complement the specific information provided in concrete cases by the companies themselves, the US authorities should strive to offer **more information in an accessible and easily understandable form to the individuals regarding their rights and available recourses and remedies.**
45. The Privacy Shield website already had a specific section named "EU and Swiss individuals" containing subsections "My rights under Privacy Shield" and "Privacy Shield participants list"¹⁹ where individuals were informed about their rights. The various possibilities to lodge complaints were also explained and partly supported by direct links. After the first annual review and as a response to the WP 29's suggestions the DoC added a one-page document to their website that gives individuals an overview²⁰ of the program with a strong focus on the individual's rights and how they can be exercised. The EDPB acknowledges the efforts made by the DoC to provide further guidance for EU individuals on the Privacy Shield website. Although the number of complaints slightly increased since the last report, it remains difficult to determine whether this is directly linked to this guidance. The EDPB will thus remain watchful.

3.3 Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism

46. After having noted improvements in the certification process in the report of the second Joint Review, the EDPB did not identify any relevant change of the procedures in the third Joint Review:
47. The DoC still reviews all self-certifications (both for first time applicants and for recertification submissions) and checks:
1. Registration with an Independent recourse mechanism (IRM) company
 2. Payment of Annex I Arbitral Fund Contribution

18 that the guidance could for example further elaborate on the following details: Notice to be provided by processors needs to be in line with the contract in place between the processor and the controller; that access to data and a Choice mechanism could be provided to the individual directly by the processor provided however that the controller has in the first place authorized the processor to do so; and that for a processor compliance with the Data Integrity and Purpose Limitation principle requires it to process the data only in accordance with the instructions from the controller and on the other hand to implement the appropriate measures as instructed by the controller to assist the later in complying with the data integrity principle.

19 See: <https://www.privacyshield.gov/Individuals-in-Europe> (last accessed on 27 November 2018)

20 See: <https://www.privacyshield.gov/servlet/FileDownload?file=015t000000QJdq> (last accessed on 14 December 2018)

- 3. Compliance with Privacy Shield supplemental principle 6 (on access to personal information)
 - 4. Completion and consistency of certification information
 - 5. Privacy notices (the existence of all 13 elements required by the Privacy Shield is checked also in the organizations Privacy Policy)
48. Also, the DoC still asks the organizations for more precise links provided for the Privacy Shield listing so individuals can more easily exercise their rights and for more than one point of contact within the organization to make sure messages from the DoC are received. The DoC also checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR).
49. When the DoC refused to list an organisation on the Privacy Shield list, either for first-time certifications or re-certifications, it underlined that it was because the requirements set out by the Privacy Shield were not fulfilled. This indicates that the decision made by the DoC whether or not to list an organization on the Privacy Shield website is – as far as the checks go - not a rubber stamp exercise.
50. However, on the basis of the information given by the US authorities during the joint reviews, those checks still do not go into the substance of the principles. **This absence of substantial checks remains a concern for the EDPB on the general question of sufficient oversight regarding the substance of the Privacy Shield principles.**
51. Following the criticism expressed by the WP 29, the DoC still prohibits a first-time applicant from making public representations about participation until the Privacy Shield Team approves its certification and instead requires an applicant to submit a draft privacy policy for review. It also directs an applicant to remove any premature references of their participation in the Privacy Shield program from their website.
52. **Regarding the re-certification process**, already the second annual review revealed that due to the procedures established by the DoC there are cases where the due date displayed on the Privacy Shield List is already passed while the organization still is listed as an active participant. This occurs when an organization has submitted their recertification but the process is not finalized before the due date. In the third review this was further explored and it was discovered that the process of recertification could take up to 105 days starting at the actual due date. During this whole period of time the organizations will stay on the “active” list.
53. As long as the organizations still publicly commit to apply the Privacy Shield Principles this might not lead to a gap in the protection of individuals. **However the EDPB reiterates that it is the reasonable expectation of individuals who consult the Privacy Shield list that all organizations listed as “active” have current and valid certification checked by the DoC. The EDPB is of the opinion that the change of practice to already set a new due date on the Privacy Shield list as soon as the recertification documents are submitted to the DoC does not lead to the result that only fully checked certifications are displayed as “active” on the List. The EDPB still asks the DoC to explore what can be done to avoid this situation (especially what can be done to guarantee that there is no gap in the protection of individuals) and in the meantime to add some explanation for concerned individuals and EU based organizations using the Privacy Shield as a transfer tool so the situation is sufficiently clear to individuals and also organizations within the EU that would like to transfer personal data to a Privacy Shield certified organization and therefore check the validity of the certification on the Privacy Shield List.**

54. During the course of the third Joint review it was also discovered that on the Privacy Shield list there were 29 Organizations listed as “active” that had a due date in 2018. **The EDPB asks the DoC to implement procedures that make sure that the “active” list of participants is always up to date and to implement checks that avoid such outdated listings.**

3.4 Oversight and supervision of compliance with the Principles – Activities of the DoC

55. In the first Joint Review report the WP 29 criticized that the **oversight of the commercial aspects of the Privacy shield mainly relied on the third party companies providing Independent Recourse Mechanisms (IRMs)** and that the **implementation** of the Privacy Shield framework **lacked sufficient oversight and supervision of compliance in practice**. Because the Privacy Shield is a program based on self-certification, it is of utmost importance that U.S. authorities involved in the administration of the Privacy Shield devote sufficient resources at oversight and enforcement activities. The WP 29 considered that the **performance of compliance reviews** of organizations having self-certified to the Privacy Shield is a key element for the effective functioning of the framework and that **ex-officio investigations have to be conducted both by the DoC and the FTC/DoT** to ensure that self-certified organizations concretely implement the requirements of the Privacy Shield.
56. The second review showed that the U.S. authorities (namely DoC and FTC) had made significant efforts to address this concern:

- On a quarterly basis the DoC conducts “false claims reviews” in order to identify organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.

The identified organizations receive a certified letter from the DoC, warning them of potential referrals to the FTC or DoT if they do not fulfil outstanding requirements or withdraw properly from the program. The DoC informs the FTC/DoT of its intent to send those letters. The organizations have 30 days to respond to the letter. The DoC compiles a list of those organizations that fail to take action and respond to the letter. This procedure has led to 100 referrals from the DoC to the FTC, 56 of those referral were made in the second year of the Privacy Shield program. DoC and FTC/DoT cooperate throughout the whole process. Simultaneously with the referral an organization is (at least temporarily) removed from the “active” Privacy Shield List.

- As foreseen in the Privacy Shield text, the DoC also performs random web searches for false claims of participation in the program. Those web-searches have only led to few cases that were referred to the FTC.
- The DoC has performed a sweep of 100 randomly chosen organizations. The focus of the sweep was the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. The DoC sent more in-depth compliance questionnaires to 21 organizations that showed minor or more significant peculiarities (for example: No response from the designated point of contact; the Privacy policy was no longer accessible online; Missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter requiring the organization to indicate within a 30-day period how it has addressed the concerns. If those are not resolved within the 30 days, the organization is moved to the “inactive” list and the case is being referred to the FTC or DoT.

- The DoC has also designated 1 person to follow the media and to do keyword searches to identify possible breaches of the Privacy Shield commitments.
 - The DoC also performs regular checks for broken links to the privacy policy on the Privacy Shield list.
57. This year, the DoC indicated that it issued more than 670 warning letters, most of them regarding false claim participation.
58. Aside from the fact that the DoC has increased the amount of random spot checks to 30 randomly chosen organizations per month, the third Joint Review did not reveal any further developments in this direction.
59. **Therefore, while the EDPB still welcomes all these steps taken by the DoC to ensure formal compliance with the Principles of the Privacy Shield because they remain a good starting point; the EDPB is deeply concerned that these checks still remain focused on the formalities to be complied with rather than on the substance. The EDPB urges the DoC to extend the oversight activities also to substantial elements, such as the purpose limitation principle for instance.**
60. Further to monitoring concrete compliance with all principles of the framework, **one of the areas that would need particular attention in this context remains the area of onward transfers.** The DoC has still not made use of its right to request a copy of the relevant privacy provisions of organizations contracts with their agents. **Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance to closely monitor the practical implementation of the Accountability for the Onward Transfers Principle.**

3.5 Oversight and supervision of compliance with the Principles – Activities of the FTC

61. In last year's review the EDPB noted an increase in the FTC's activities regarding the enforcement of the Privacy Shield. This year however, the FTC recognized that due to its lack of budget, it had to prioritize its actions with regards to the enforcement of Privacy rules.
62. While last year the FTC has brought 5 new Privacy Shield cases: 2 against organizations that did not complete their certification and 3 cases where the certification has lapsed. In most of those cases, the organization failed to verify the deletion, return or continued application of the Privacy Shield Principles to personal data transferred under the Privacy Shield. The FTC indicated that some investigations into potential Privacy Shield violations remain ongoing, without further clarifying their scope and the exact number of cases. This year the FTC has brought 7 new cases regarding the enforcement of the Privacy Shield, still on administrative failures and not on the substance of the Privacy Shield's principles. The EDPB stresses that further controls concerning onward transfers could be led, given that the solutions put in place by the certified companies are not checked by the DoC either.
63. In the Division of Privacy and Identity Protection, Bureau of Consumer Protection there are 40 lawyers almost exclusively working only on privacy. They are supported by for example technical experts.
64. The FTC investigates Privacy Shield-related referrals (143 discovered "false claim cases" in the third year) but in most cases by the time these referrals arrive to the FTC they have been solved in the meantime so many cases fall out.

- 65. Concerning the Facebook settlement reached since last year's joint review, the FTC clarified that the scope of it remains outside the scope of the Privacy Shield as none of the products covered by the settlement were certified under the Safe Harbor or the Privacy Shield²¹.
- 66. **The EDPB still welcomes any ex officio activity to proactively monitor compliance with the Privacy Shield Principles undertaken by the FTC. It nevertheless regrets the low number of cases concerning the enforcement of the Privacy Shield and that the FTC still was unable to share any more detail on its approach as this leaves the EDPB unable to have a clear insight on the concrete activities and cases, and therefore to be in a position to assess how and to what extent the FTC ensures compliance monitoring with the substance of the Privacy Shield's principles.**

3.6 Independent Recourse Mechanisms

- 67. The independent dispute resolution providers reported an overall increase in both the number and complexity of the complaints received under the Privacy Shield framework since the second joint review. The EDPB acknowledges that the number of complaints slightly raised and were resolved in a timely manner. However, the increase of complaints in general do not entirely compensate for the lack of proactive checks from the competent US authorities. Indeed, from the feedback collected during the Joint Review, the complaints do not seem to concern the issues of concerns underlined by the EDPB so far as they seem to mainly focus on procedural aspects.
- 68. In the report of the second annual joint review, the EDPB expressed its expectation to see improved and comparable reports provided by the IRM services that also explain how possible conflicts of interests are precluded. The DoC reported that it has developed guidance to the IRMs in order to avoid possible conflicts of interests, and updated its guidance on Annual IRM report to include potential conflicts of interest and the description of how they avoid such situations. However, the guidance developed and standardized forms issued do not cover all aspects of the reports. In particular, the EDPB found that no standardised template format for the reports have been introduced yet on this aspect. In order to ensure full comparability, the EDPB therefore recommends the DoC to introduce a standardized template format for the Annual IRM report, which also contains explanation on how possible conflicts of interests are precluded.

3.7 HR Data

- 69. As already stated in the previous reports, the notion of HR data in the context of the Privacy Shield is interpreted differently within the EU and by the US authorities. Although the DoC initiated the producing of guidance regarding the processing of HR data, including through informal consultation of members of the WP 29 and of the EDPB later on, on working level in this regard, the work on this guidance was not successful yet due to the absence of convergence on the definition of the notion of HR data. Last year's review thus focused less on the definition of HR data but rather on the consequences, the different definitions within the EU and by US authorities may lead to. On the EU side, the concern is that additional protections granted by the Privacy Shield for employment data (opt-in to marketing purposes rather than opt out) would not and could not be enforced by any U.S or EU authority. The EDPB recalls that in its understanding, HR data should be protected in the same way whether they are processed by the employer or by a processor, including concerning the choice and

21 The effects of the immunity of the settlement reached however remained unclear. Indeed, this immunity would not prevent individuals to bring actions against Facebook for other products, or for practices which were unknown at the time of the settlement. However, should Facebook adhere to the Privacy Shield in the future for the products covered by the settlement, without changing anything from its commitments, it is still to be clarified whether the immunity derived from the settlement would cover corresponding violations of the Privacy Shield in this context for the practices covered by the settlement.

purpose limitation principles. While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. **In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations lead to gaps in the protection of employees in the European Union.**

3.8 Automated-decision making/Profiling

70. In the report of the first annual review, the WP29 called upon the Commission to contemplate the possibility to provide for specific rules concerning automated decision making to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis, especially after having explored the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies if the analysis generates an actual need for additional safeguards.
71. As part of the second review the Commission presented the main elements of a study²² commissioned to an independent contractor regarding the existence of automated decision-making on the basis of personal data that has been transferred from the EU to Privacy Shield certified companies in the US. While the authors of the study highlight a series of challenges for conducting this work (limited availability of experts on the topic and reservations to take part in interviews, limited relevance of answers in certain cases, opacity characterizing the data industry on such practices notably), the main conclusion that can be drawn from the study is that automated decisions (in the narrow GDPR definition of decisions having legal effects on individuals or similarly significantly affecting them) are not taken on the basis of data transferred from the EU. According to the study, such decisions are more likely to take place in “EU customer facing” situations (i.e. where the US company directly targets EU customers).
72. However, the study at the same time underlined that this is a fast developing area which still has to be closely monitored in the future, therefore this issue was also discussed at the third annual joint review.
73. In their reply to the questionnaire sent by the Commission in preparation to the third joint review, one trade association reported that member companies that employ automated decision-making included information about this in their policies and maintain mechanisms to allow consumers to exercise control, such as the ability to contest an automated decision and seek human review.
74. During the third joint review, the FTC confirmed that the U.S. adheres to the OECD Recommendation on AI [adopted on 22 May 2019].
75. The FTC specified that companies are not required to provide the right to know the logic involved and to request reconsideration on a non-automated basis under the Privacy Shield (and therefore, to include a reference in this regard in the privacy policy submitted pursuant to the Privacy Shield). If companies do commit themselves to provide these rights, but then, contrary to this commitment, they do not provide them, this will constitute a misrepresentation, against which the FTC can take enforcement action. In the area of consumer credit, the FTC referred to the Fair Credit Reporting Act (FCRA).
76. **Based on the findings of the third joint review, the EDPB is on the opinion that it is important that the Commission continues monitoring cases related to automated decision making and profiling and**

22 See: https://ec.europa.eu/info/sites/info/files/independent_study_on_automated_decision-making.pdf (last accessed on 19 December 2018)

to contemplate the possibility to foresee specific rules concerning automated decision making to provide sufficient safeguards, including the right to know the logic involved and to challenge the decision obtaining human intervention when the decision significantly affects him or her.

4 ON THE DEROGATIONS TO THE PRIVACY SHIELD TO ALLOW ACCESS TO DATA FOR LAW ENFORCEMENT AND NATIONAL SECURITY PURPOSES

4.1 Introduction

77. **Since the second Joint Review, the US legal framework has not substantially changed.**
78. Consequently, some of the main points of concern that the WP29 and the EDPB expressed in their previous opinions, in the area of access to data transferred under the Privacy Shield for national security or law enforcement purposes, have not been fully resolved. These **main concerns are related to the collection of data, to oversight, to judicial redress and finally, to the Ombudsperson mechanism. This calls for a reminder of the EDPB's analysis.**
79. **In addition,** this year's joint review took place at the time the "Schrems II" case, also concerning the Privacy Shield, is pending before the CJEU (the Court held the hearings on this case on 9 July 2019).
80. Also taking this background into account, specific points were discussed with the U.S. authorities during the Privacy Shield Review (*See infra*, in particular concerning PPD28, when data are collected outside the US).

4.2 Collection of data (under section 702 and under EO 12333)

81. As recalled in the previous reports, the CJEU underlined in its Schrems judgment²³ that the "*protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary*"²⁴ and ruled that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter*"²⁵.
82. **The previous concerns expressed therefore remain relevant**, as the legal framework has not significantly changed on any of the aspects concerning the collection of data from the perspective of EU individuals (and non-US persons). Therefore, the EDPB recalls the concerns expressed in this respect in the two previous reports.

4.2.1 Collection of data for national security purposes under Section 702

83. The EDPB stresses once again the need for independent assessment on the necessity and proportionality of the definition of "targets" and of the concept of "foreign intelligence" under section 702 FISA (including in the context of the UPSTREAM program), and maintains its call for further independent assessment of the process of application of selectors in specific cases ("tasking of selectors"). It also maintains its call for further clarification in the context of the UPSTREAM program to exclude that massive and indiscriminate access to personal data of non-U.S. persons takes place.

23 Case C-362/14, 5 October 2015

24 See recital 92, See also cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger, recital 52.

25 See recital 94.

- 84. With regard to 702 FISA, it was clarified during the discussions of this year's Review that a "person" to be identified as a target could refer to several individuals using the same identifier, provided that all these individuals would be non-U.S. persons and fulfill the applicable criteria for being targeted²⁶.
- 85. **The EDPB welcomes that the now fully functional Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency, has decided "to review the FBI's querying (searching) of data obtained pursuant to Section 702" as well as the fact that the PCLOB indicated it would follow-up how the previous recommendations expressed in their report concerning section 702 were taken into account. However, it regrets that PCLOB does not intend to prepare and issue an updated general report on Section 702, building on the report issued in 2014, especially given that since then section 702 was reauthorized. A general updated report would help provide an assessment of the new provisions inserted in Section 702 in the context of its reauthorization, as well as on the practice of other agencies than the FBI, in particular intelligence agencies.**

[4.2.2 Collection of data for national security purposes under Executive Order 12333](#)

- 86. **In the context of the third Joint Review, given the disagreements between the EDPB and the US authorities as to the relevance of Executive Order 12333 for the adequacy decision, the application of Executive Order 12333 was still not further discussed.**
- 87. As underlined in the previous reports, the EDPB maintains the WP29 long-standing position that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third country's law which allow it to conduct surveillance outside its territory as far as EU data are concerned. Necessary limitations to governmental access to data should extend to personal data "**on its way**" to the country, for which adequacy is recognized. The EDPB recalled this position before the CJEU²⁷. During the previous Joint Reviews, the U.S. authorities underlined that Executive Order 12333 could not be used as a basis for collection of data inside the U.S. territory and that they consider that collection of data under this Executive Order falls outside the scope of the Privacy Shield.
- 88. Once again, given the uncertainty and unforeseeability of how EO 12333 is applied, the EDPB stresses the importance of the awaited PCLOB's reports on this text. However it understands that they are likely to remain classified, so that no further information on the concrete operation of this Executive Order and on its necessity and proportionality would become available neither to the public, nor to the Review team of the EDPB.

[4.2.3 Safeguards provided in Presidential Policy Directive 28 \(PPD-28\)](#)

- 89. The U.S. authorities confirmed once again their commitment to comply with the rules set in the Presidential Policy Directive 28 (PPD-28). The EDPB welcomes this commitment. At the same time, the EDPB stresses that the PPD-28 provides for the only safeguards and limits to the collection and use of data collected outside the U.S., as the limitations of FISA or other more specific U.S. law do not apply. These limitations mainly concern the collection of data, as the signal intelligence activities have to be as "tailored as feasible".
- 90. **No new substantial discussion took place in the context of the third joint Review, concerning the interpretation and application of the six purposes allowing for the use of data foreseen in this Directive, or relating to the amount of personal data collected by the U.S., that would allow a validation**

26 For instance, this could cover for a couple using the same email address or the members of an organization using the same communication app account.

27 At the hearing organised on the 9 July 2019 in the so-called Schrems II case (C-311/18)

of the commitments and the assurances provided by U.S. authorities. In the context of this year's Joint Review, discussions mainly focused on the interpretation and application of the additional ground (situation/scenario) for bulk collection foreseen by the first sentence of footnote 5 of Section 2 PPD-28²⁸, which provides that "*The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection.*" The U.S. authorities explained the meaning of "*signals intelligence data that is temporarily acquired to facilitate targeted collection*". The EDPB understood from these discussions that this footnote means that data may be collected in bulk - and regardless of the six purposes foreseen in Section 2 - if collected temporarily, with a view to establishing an identifier for a defined target. This would thus be an additional ground to collect data in bulk, and in this case general principles of Section 1 of PPD-28 would still apply. The EDPB regrets that the notion of "temporarily" could not be further specified, as in the EDPB's understanding, it appeared to mean that as long as the target has not been identified, bulk collection could continue.

91. The EDPB also recalls that a more detailed follow-up report on how the key terms of the PPD-28 are practically understood and applied in the different surveillance programs would be welcome, since it could provide additional information clarifying these aspects.
92. In addition, although the U.S. authorities claimed that Executive Orders and Presidential Policy Directives have "the force of law", the EDPB recalls that in the context of the previous Joint Reviews, it was also clarified that these violations of the instruments can never be - in themselves - relied upon for an action by an individual before a Court. Therefore, it would not be possible for an EU individual to directly invoke the violation of PPD-28 safeguards to bring an action before a U.S. Court.

4.3 Oversight

93. The EDPB recalls that comprehensive **oversight of all surveillance programs** is crucial, which the CJEU and the ECtHR have also emphasized in the respective jurisprudence.
94. Already during the two previous annual Joint Reviews, the oversight activities of several entities were presented. The EDPB considered that a **comprehensive oversight structure** is in place, composed of different elements that are in part, independent from the Intelligence Community, including the Privacy and Civil Liberty officers, the Inspector Generals, the PCLOB, the FISC and Congress, amongst others.
95. **The EDPB welcomes the appointment of the last missing members of the PCLOB. The PCLOB is now fully functioning and operational. The PCLOB also presented, for the first time, its work program, and the EDPB welcomes this step in terms of transparency from this oversight body.** As emphasized before, the EDPB considers the PCLOB, whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been particularly helpful to understand the functioning of the various programs, as an independent body, an essential element of the oversight structure. The EDPB calls again for public reports to be published, including on crucial aspects of the U.S. legislation such as the three reports (one of which only is already finalized) on EO 12333, especially since the functioning of this piece of legislation could never be discussed during the joint reviews. In this context, the EDPB also regrets that, although the PCLOB indicated it would follow-up how the previous recommendations expressed in their report concerning section 702 were taken into account (see supra as well), no general updates of previous reports will be prepared, be it on Section 702 FISA or on PPD-28. Furthermore, the EDPB recalls that in the context of joint reviews organized for other EU instruments such as for PNR agreements or for the TFTP agreement, members of the Review Team are

28 Which applies only to Executive Order 12 333 and not to Section 702 FISA, which does not allow bulk collection.

given access to more information than the general public. However, in the case of the Privacy Shield joint reviews, the members of the review team only have access to the same documents as the general public. They recall that they remain ready to review additional documents and discuss additional elements under security clearance, in order to have more meaningful reviews.

4.4 Redress for EU individuals

96. As already highlighted in the previous reports, the EDPB underlines that in its Schrems ruling, the CJEU stressed the importance to have a right to an effective remedy before a tribunal²⁹. A third-country can only be considered as providing an adequate level of protection in accordance with the GDPR, where EU individuals have access to an independent and impartial redress body, including in surveillance matters.
97. **As the U.S. government informed during this year's Joint Review that the legal framework is unchanged and no significant new case law concerning these matters needed to be considered, the EDPB recalls its position and the relevant criteria to take into account when assessing the level of adequacy are still those stemming from the jurisprudence of the CJEU and ECtHR.**
98. As repeatedly stressed in the previous reports, while the APA and FISA appear to provide limited grounds for an EU individual to challenge surveillance in U.S. courts, the principal problem appears to concern the “standing requirement”.
99. Under the procedural requirements as currently interpreted by the U.S. courts, it appears to be difficult and uncertain that an EU individual could satisfy the procedural requirement of standing when bringing a suit concerning a surveillance measure on the basis of section 702 FISA or EO 12333. The EDPB will therefore continue to follow closely the evolution of these cases as they could trigger the establishment of new additional guarantees having a positive impact on the effectiveness of judicial redress offered to EU individuals before U.S. courts. However, as was confirmed during the Joint Reviews, the interpretation of the notion of “standing” in surveillance matters is evolving with cases still pending³⁰.

4.5 Ombudsperson mechanism

100. **In the context of the third Joint Review, the EDPB welcomed the nomination of Mr Keith Krach, on 18 January 2019, as “permanent” Ombudsperson**
101. The **Ombudsperson** mechanism aims at complementing the possibilities of redress. More critically, it might be argued that it is meant to compensate for the uncertainty or unlikelihood to seek effective redress before a U.S. court in surveillance matters. The WP29 therefore welcomed the establishment of the Ombudsperson, as this could constitute a significant improvement in terms of protection of the rights and freedoms of EU individuals with regards to U.S. intelligence activities. In addition, it was confirmed that the PPD-28 does not create enforceable rights for the individuals (see *supra*). The Ombudsperson mechanism provides the only way for EU individuals to ask for a verification that the relevant authorities have complied with the requirements of this instrument by asking the Ombudsperson to refer the matter to the competent authorities, which include the Inspector General, to check the internal policies of these authorities.
102. Having regard to Article 47 of the Charter of Fundamental Rights of the European Union, the threshold for independence and impartiality required in a redress mechanism such as the Ombudsperson is high.

29 See paragraph 95

30 See in particular cases *ACLU v. Clapper*, and *Wikimedia v. NSA*.

Having analysed the jurisprudence of the ECtHR in particular, the WP29, in its Opinion of 13 April 2016, and the EDPB assessed the Ombudsperson mechanism in their opinions and in previous reports, and suggested that the appointment of a high-ranking official in the Department of State as the Ombudsperson, who can be dismissed at any time without notice, is problematic having regard to aforesaid requirements of independence and impartiality³¹. This concern is also raised by the designation, as Ombudsperson, of Mr Keith Krach, given the fact that he is the Under Secretary of State for Economic Growth, Energy, and the Environment.

103. In addition, the EDPB recalls that during the first and the second Joint Reviews, as well as before the EDPB Plenary in July 2018, the previous Ombudsperson and the U.S. government explained in some detail the important work done in order to ensure that requests would be handled lawfully and efficiently. The previous Ombudspersons also stressed that they needed to be convinced of the findings before responding to the request and underlined that they could escalate the issue should they be unconvinced by the outcome presented to them following the assessment of a request. These aspects were confirmed by the new Ombudsperson, who also underlined his personal commitment to only sign letters to close cases when convinced that they had been dealt with in a proper way. While the EDPB still has no reason to doubt the integrity of the new Ombudsperson, **it recalls its expectation to learn more about the powers of the Ombudsperson vis-à-vis the Intelligence Community**. This information still remains partial. The procedures governing the access to relevant information by the Ombudsperson and governing the interactions of the Ombudsperson with the other members of the Intelligence Community, including the oversight bodies, remain partially classified.
104. As the first case referred to the Ombudsperson mechanism since the second Joint review was eventually declared inadmissible because it concerned data transferred outside the scope of the Privacy Shield, the case has not allowed to further discuss in detail how cases are handled under the procedures in place after the preliminary assessment of the admissibility of a case.
105. Nevertheless, the staff of the Office of the Ombudsperson explained in abstract how an admissible case would be handled. In this context, it was explained that violations of Section 702 FISA would also be reported to the FISC, which may decide to issue deficiency order to have it remedied within 30 days.
106. Questioned about his role in the Ombudsperson mechanism, the Inspector General for the Intelligence Community (“IG”) confirmed that the first complaint sent to the Ombudsperson was shared with him, and that more generally in the context of requests sent by the Ombudsperson, he would, depending on the circumstances of the case, refer it to the competent intelligence agency, and that a remedy could be proposed to the ODNI. It was recalled that in case of an acknowledged incident, collection stops, the underlying information has to be purged, and, if any reports were based on that information, these reports must be recalled (this is a standard procedure for reports in this domain). He added that Congress would also be informed about recommendations and about cases where the recommendation is not followed through. Further, the IG explained that the Ombudsperson would also be informed of the findings and recommendations to the ODNI necessary for the Ombudsperson to perform his duties. Nevertheless, the IG confirmed that in his report to the Ombudsperson, he could remove information from the report to the ODNI in order to protect sources and other sensitive information. As a consequence, the information shared with the Ombudsperson may not necessarily be identical to the information shared with the ODNI.
107. With regard to the first case under the Ombudsperson mechanism, the EDPB is committed to assess its internal processes in light of the experiences made and to adapt them, if need be.

³¹ See WP29 Opinion ‘European Essential Guarantees’, Guarantee C, referring among others to ECtHR, Zakharov.

108. In conclusion, based on the available information, the EDPB still doubts that the powers of the Ombudsperson to remedy non-compliance vis-a-vis the intelligence authorities are sufficient, as his “power” seems to be limited to decide not to confirm compliance towards the petitioner. In the understanding of the EDPB, the Ombudsperson is not vested with powers, which courts or other similarly independent bodies would usually be granted to fulfill their role. Therefore, the EDPB remains unable to hold that the Ombudsperson is vested with adequate powers to effectively exercise its duty. In addition, the EDPB recalls that the decisions of the Ombudsperson cannot be brought to court for judicial review. Therefore, the lack of judicial review of the decisions of the Ombudsperson, and consequently the impossibility to obtain remedies where the Ombudsperson will not provide any answer (failure to act) or provides an unsatisfactory reply to the complainant, still remains a concern. **As a conclusion, the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient independence, and with sufficient powers to access information and to remedy non-compliance. Thus, it cannot state that the Ombudsperson can be considered an “effective remedy before a tribunal” in the meaning of Art. 47 of the Charter of Fundamental Rights³².**

4.6 Access to data for law enforcement purposes

109. As regards **access to data for law enforcement purposes**, the EDPB continues to note that the procedural safeguards inherent to the criminal procedure (notably, due process) imply that data are accessed by the competent public authorities for a specific purpose and that the individual concerned is notified if her or his data have been accessed within the framework of a criminal proceeding, in the context of which they can raise objections to the collection and use of such data and have access to judicial redress.
110. However, the EDPB recalls the concerns - already expressed in the previous opinion issued by the WP29³³- regarding the availability of effective remedies to the individuals concerned in cases where the data processed by companies is accessed by law enforcement authorities³⁴.

5 CONCLUSION

111. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially ex officio oversight and enforcement actions, as well as the appointments of the last missing members of the PCLOB and of a permanent Ombudsperson.**
112. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities.**
113. **As regards the commercial aspects, the absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR data and the application of the principles when it comes to processors, as well as the recertification process. More generally, the members of the Review Team would benefit from a broader access to non-public information, concerning commercial aspects and ongoing investigations.** In addition, the EDPB recalls the **remaining issues with respect to certain**

32 A first request from an EU individual was received under the Ombudsperson mechanism at the end of 2018.

33 See WP 238.

34 Concerning access to data for law enforcement purposes, we also pointed out, supra, at Section 2.1 of this Report/Conclusions, to the possible access (querying) by law enforcement authorities to data acquired under Section 702 FISA.

elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.

114. As regards the **collection of data by public authorities**, the EDPB can only encourage the PCLOB to issue and publish further reports. It regrets that on Section 702 FISA no general report is contemplated, to provide an assessment of the changes brought since the last reauthorization in 2018. **The EDPB would be very interested on an additional report on PPD-28 to follow up on the first report** including an assessment of how the safeguards of PPD-28 are applied. Finally, the EDPB underlines the importance of reports on Executive Order 12 333, and regrets that those reports will most likely remain classified. In this regard, the EDPB stresses that the members of the review team only have access to the same documents as the general public. **The EDPB recalls that the security cleared experts of the EDPB remain ready to review additional documents and discuss additional classified elements**, in order to have **more meaningful reviews**, following the example of PNRs or TFTP reviews.
115. **On the Ombudsperson mechanism**, despite some new elements provided during this year's review, especially on the procedural aspects in relation to the first case submitted to the Ombudsperson but declared inadmissible, as well as on hypothetical cases, **the EDPB is still not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Thus, it still cannot state that the Ombudsperson can be considered an “effective remedy before a tribunal” in the meaning of Art. 47 of the EU Charter of Fundamental Rights.**
116. Finally, the EDPB recalls that the **same concerns will be addressed by the Court of Justice of the European Union in cases that are still pending before it.**

ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW

Factual findings of the third annual joint review of the EU-US Privacy Shield

GENERAL INFORMATION

1. The U.S. Delegation was composed of high level representatives.
2. As of now, the Privacy Shield List contains around 4984³⁵ organizations, 509³⁶ are on the “Inactive” List either because they have voluntarily withdrawn from the program (39 in the last year), not submitted their recertification in a timely manner or because their recertification has been initiated but not completed in a timely manner. There was no case where an organization was removed from the List because it persistently failed to comply.
3. Of the participating Organizations 70 - 75% are small and medium size organizations with less than 250 employees. 96% of the participating organizations certified for non-HR data transfers, 33% for HR transfers. The main businesses certifying are: Information and Communications Technology, Business and Professional Services, Media and Entertainment, and Education.

1 ON COMMERCIAL ASPECTS

1.1 Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program

4. The DoCs method and scope of checks in the initial review of a certification and the recertification has not changed substantially since the last review. The DoC reviews all self-certifications (first time applicants as well as recertification submissions) for:
 1. Registration with IRM
 2. Payment of Annex I Arbitral Fund Contribution
 3. Compliance with supplemental principle 6
 4. Completion and consistency of certification information
 5. Privacy notices
5. DoC has rejected 9 first time certifications in the last year because the applicants were not eligible to participate in the Privacy Shield because they were not under the jurisdiction of FTC or DoT (5 non-U.S., 4 non-profit organizations).
6. Also, there were no significant changes reported as regards the depth of the analysis the DoC performs: the DoC checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR). It does not check if the data transferred is necessary and proportionate to the purpose for instance because they consider that the Privacy Shield does not go into this level of detail, nor do they check in substance the compliance with other principles.

³⁵ See <https://www.privacyshield.gov/list> on 24 September 2019

³⁶ See <https://www.privacyshield.gov/inactive> on 24 September 2019

7. In order to address the concern expressed by the WP29 regarding the duty of the certifying organization to publish their privacy policy referring to the Privacy Shield certification before the DoC has completed the exercise of checking and listing the organization, the DoC has changed the procedure.
8. The DoC:
 - Prohibits a first-time applicant from making public representations about participation until the PS Team approves its certification
 - Requires an applicant to submit a draft privacy policy for review
 - Directs an applicant to remove any premature references
9. As the practical experience with the certification process increases, the DoC still uses the same guidance for the review of applications regarding the identification of foreign entities; they ask the companies for more precise links to their privacy policies so individuals could more easily exercise their rights, they ask for more than one point of contact within the organization to make sure messages from the DoC are received.
10. In addition to the 2-weeks-notice of the upcoming deadline to recertify organizations already sent out before the second annual review, the DoC now also sends a reminder one month and one week before the recertification is due.
11. The organizations that want to stay in the Privacy Shield program are obliged to communicate their re-certification by the due date. The DoC stated in the third annual review that organizations that fail to do so within 30 days after the due date are “automatically” moved to the “inactive” list.
12. Since August 2019 the DoC has changed their practice and changes the “Next Certification Due Date” on the Privacy Shield list as soon as any documents for recertification arrive at the DoC.
13. In the course of the 3rd annual review the participating representatives of the EDPB submitted a list of organizations whose recertification due date lay in the past. For 29 of those organizations the due date dated back to 2018. Checks of that list performed on September 25, 2019 led to the result that the DoC moved 87 of those organizations to the “inactive” list. Two organizations disappeared from the whole list. 213 remained on the “active” list.
14. As regards guidance, the DoC has published new guidance material for organizations to address questions around Brexit. The review team is not aware that this guidance was created in cooperation with EU SAs or the EDPB.

1.2 Oversight and supervision of compliance with the principles - Activities by the DoC

15. The DoC still identifies on a quarterly basis organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.
16. If organizations do submit the paperwork necessary for recertification, the DoC foresees a timeslot of 45 days in which the recertification should be finished. If this is not the case and at least further action to complete the process is not taken by the organization, the DoC sends it a warning letter explaining that if the required action is not taken within a period of another 30 days, the organization will be removed to the “inactive” list and referred to the FTC or DoC.

17. As foreseen in the Privacy Shield text, the DoC still performs random web searches for false claims of participation in the program.
18. In the last year the DoC referred 143 discovered false claims cases to the FTC.
19. After the DoC has performed a sweep of 100 randomly chosen organizations in the second year of the Privacy Shield, it has now started in April 2019 to perform 30 of those checks each month. The focus of the sweep is the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. In case those checks result in conspicuities (about 20% of the cases) the organizations receive more in-depth compliance questionnaires from the DoC. Through this procedure minor or more significant peculiarities may appear (for example: no response from designated point of contact; privacy policy was no longer accessible online; missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter (3 in this year) requiring the organization to indicate within a 30 day period how it has addressed the concerns. If those are not resolved within the 30 days the organization is moved to the “inactive” list and the case is being referred to the FTC or DoT. It was confirmed that even if the case was resolved within the 30 days the DoC could refer it to the FTC.
20. In total the DoC has sent out 669 warning letters to participants of the Privacy Shield since October, and 1 100 were sent in total since the beginning of the programme.
21. The DoC still follows the media and does keyword searches to identify possible breaches of the Privacy Shield commitments.
22. The DoC also still performs regular checks for broken links to the privacy policy on the Privacy Shield list.
23. The DoC has still not made use of its right to request a copy of the relevant privacy provisions of an organizations contract with an agent.
24. Besides the Privacy Shield News and Events section on the website of the DoC that covers several kinds of news and also FTC decisions related to privacy in general but there is no dedicated link to Privacy Shield cases of the FTC as described in the text of the Privacy Shield.
25. In relation to the DoC’s work in order to ensure that all organizations recertify and finish their work on time but also for the web searches for false claims and any other aspects of their work the DoC mentioned that it works on improving their technical possibilities.
26. The DoC has in various contexts throughout the review also uttered its wish to establish a closer cooperation between the DoC and the EDSA/ representatives of European Supervisory Authorities (for example on outreach and education, possibilities of more substantial checks).
27. The US CIB announced that they would stop managing the fund set up (to cover the costs of the EU informal panel responsible to take care of complaints submitted mostly from employees whose data have been transferred under the Shield) in accordance with the Privacy Shield in 2020. EU Commission and DPAs were approached to help finding a solution but declined any responsibility in managing it.
28. **European Commission and EDPB representatives’ presentations** The European Commission, EDPB Chair and representatives gave a short presentation on the updates about the work done on the European Union side.

1.3 Independent Recourse Mechanism (IRM)

29. The DoC reported that it has developed guidance to the IRMs in order to avoid possible conflicts of interests.
30. One IRM explained once again that such a conflict of interest would be avoided by separating the teams providing IRM services and those verifying ex officio compliance with the Privacy Shield framework, both in terms of tasks and staff. Regarding the management of such potential conflicts between the two teams, it reported on having its own department that monitors these conflicts and has not had identified any so far.
31. Potential conflicts of interest must be included in the annual reports of the IRMs, but neither this aspect of the report was standardized nor any standardised template format for the reports have not been introduced yet.
32. In total, the IRMs received 48 complaints under the Privacy Shield framework and reported an overall increase in both the number and complexity of the complaints.
33. However, the IRMs reported that only one-third of the received complaints were eligible under the Privacy Shield. The other complaints were primarily regarding U.S. companies that were not self-certified under the Privacy Shield framework.
34. The majority of the complaints received were related to requests from individuals regarding a change or removal of their personal data, an unsubscribe from the organization's services, the disabling of accounts and the contact with a representative from the applicable organization.
35. Another IRM reported that three complaints were successfully resolved, which related to the access principle as well as the improper handling of the notice principle.

1.4 Arbitral Panel

36. The fee that according to the Privacy Shield text is collected from the certified organizations annually is still being collected only once at the initial certification. The collected amount (under Safe Harbor and the Privacy Shield) totals to more than 5 million \$.
37. Regarding the arbitral panel procedure, two requests were submitted since the second annual review. Both requests were dismissed as one failed to comply with the steps needed to invoke such an arbitral panel procedure and the other one did not relate to a company that was a Privacy Shield participant.

1.5 Oversight and supervision of compliance with the principles - Activities by the FTC

38. The FTC representative answered the questions of the Commission and the EDPB along the following 3 main categories:
 - 1.5.1 Concerning the status of the Privacy Shield enforcement in general
39. 7 Privacy Shield cases were handled since the last review, to look more into substantive violations of the framework.
40. Two cases concerned the supplemental principle 6 (on the obligation to continue to apply the Privacy Shield to the data collected after withdrawal from the programme). The FTC also focused on supplemental principle 7 (obligation to verify or certify that the company has assessed its compliance with the Privacy Shield).

41. The FTC also performed *ex officio* reviews: 1 case this year, where the company did not comply with this principle 7 (and thus probably with others). The representative of the FTC announced more cases on the Privacy Shield to come.

42. Following a question from the Commission, the FTC answered that it did not focus only on the formal respect of the Privacy Shield, but also on the substance.

1.5.2 On the Facebook case which led to the recent settlement with the FTC (follow-up of the discussions in the second Joint Review and update on this case)

43. Although the representative of the FTC underlined that they could not share much details as the findings have not been made public, it was indicated that eventually the investigation focused on products for which Facebook did not certify under the Privacy Shield (Facebook only certified for two new products, Workplace premium and Ads Measurement). Thus, contrary to what was expected during the second review of the Privacy Shield, the settlement reached does not have a direct link with the Privacy Shield.

44. The FTC clarified that as an effect of the settlement and of the immunity deriving from it, in the future it could only take action against Facebook concerning violations which were unknown at the time of the settlement (for instance, a new complaint on a new subject or concerning a different service). This means that if Facebook adhered to the Shield for these products without any further change, the FTC would probably not be in a position to act and that existing complaints on the aspects covered by the settlement will not be handled further.

45. Concerning the possibility for the FTC to contemplate a repetitive practice, for instance in terms of the exercise of rights of data subjects, as a persistent failure to comply, the DoC indicated that it is a possibility if an organization regularly fails to comply and it is no longer possible to assume that it is limited to an individual case.

46. Questioned about the settlements in general, the FTC indicated that it had to offer the company the opportunity to settle in all privacy cases, when the FTC is ready to open a case before the court. The FTC could refuse to settle, for instance when they have civil penalty. However the FTC would not impose a fine that would make the company go bankrupt. When calculating the amount of money for the settlement, the FTC would have to take into account how much the company earned from its practice and add the amount of the fine, according to the principle that a company shall not profit from its misconduct.

47. For each civil penalty, the FTC underlined that it was required to look at multipliers: degree of guilt, the ability to pay, deterrence and harm to consumers.

48. Concerning the interactions of the FTC with the DOJ in the context of settlements, the FTC stressed that it does not have the power to impose a civil penalty on its own and that in such situation they would have to refer the case to the DOJ, which then has 45 days to either take the case or let the FTC take it back. In case the DOJ takes the case on behalf of the State, the FTC underlined that they usually follow the recommendations made by the FTC.

1.5.3 On the general developments in US privacy law that may affect the Privacy Shield and on the resources of the FTC

49. The representative of the FTC underlined that the Federal Trade Commission's policy is to be aggressive towards companies within the boundaries of the powers they have (i.e., in cases for which the FTC is able to impose civil penalties).

50. Several cases were initiated or finalized this year.

51. The FTC is also continuing its hearing process to improve their orders. This process already resulted in the additional requirement to companies to have their assessor for outside compliance reviews approved. These assessors are also required to provide the FTC with all the documents in their possession.
52. Nevertheless, the FTC stressed its lack of effective means to perform its duties and missions (lack of resources, restricted competence and powers, e.g. with respect to non-profit organisations, etc). In this regard, it was underlined that without further resources, the FTC would not be in a position to process more than 7/8 cases regarding the enforcement of the Privacy Shield per year (although the duration of investigations vary from one case to another). The FTC is continuously advocating for a stronger law on first-time violations, the ability to reach non-profit entities, and for more resources.
53. Questioned on its investigatory powers, the FTC confirmed that they could have access to source codes with the issuance of subpoenas. Regarding the criteria used to prioritize their investigations, the FTC indicated that they try to maximize the yield of their resources. They do not plan “fishing expeditions” in advance, but prefer to collect information from open sources that may make a case. It sets its priority on cases regarding sensitive information (credit, finance, health, children information). The FTC stressed that, in principle, they are not an examination agency. Consequently, they could but do not usually investigate on-site but rather use documentation and interrogatories.

[1.6 Oversight and supervision of compliance with the principles - Activities by the DoT](#)

54. The DoT is in charge of the supervision of data processing related to air transportation, which includes two main entities: airline companies, and ticket agents. To date, no airline company is participating in the Privacy Shield, and only very few ticket agents.
55. Because the situation of DoT is very similar to that of the FTC, it looks closely at FTC’s practice and case law. The DoT has not received any Privacy Shield related complaints so far.

[1.7 Onward Transfers](#)

56. The representatives of DoC underlined that FAQs on how to comply with the Accountability for Onward Transfers Principle, published before the second review, are available on the Privacy Shield website. They contacted law firms, consultancy agencies and other stakeholders to seek more information about their experiences and expectations regarding this issue. These organizations indicated that the negotiation of the clauses on onward transfers are usually part of a wider, general negotiation, in which not only the Privacy Shield principles, but US state law also has to be considered (e.g. existing state law requirements on data breach). According to the information gathered as a result of this outreach, the organizations found the FAQs helpful.
57. The DoC does not get specific questions from organizations on onward transfers during the certification and re-certification process, applicants usually have more general questions on the interpretation of the Privacy Shield Principles.
58. Questioned about DoC’s possibility to request a summary or copy of the contract used by an applicant to comply with the principle on onward transfers, the representatives indicated that they did not make use of this possibility so far. The DoC also indicated that it is not part of the compliance questionnaire and the sweep checks to verify specifically these contracts, and the compliance with the Accountability for Onward Transfers Principle.

[1.8 Automated decision-making/Profiling](#)

59. The FTC confirmed that the US adheres to the OECD Recommendation on AI [adopted on 22 May 2019].
60. In their reply to the questionnaire from the review team, one trade association reported that member companies that employ automated decision-making included information about their policies and maintain mechanisms to allow consumers to exercise control, such as the ability to contest an automated decision and seek human review.
61. The FTC specified that companies are not required to provide such rights under the Privacy Shield (and therefore, to include a reference in this regard in the privacy policy submitted pursuant to the Privacy shield). If companies commit themselves to provide these rights but then, contrary to this commitment, they do not provide them, this will constitute a misrepresentation, against which the FTC can take enforcement action.
62. In the area of consumer credit, the FTC referred to the Fair Credit Reporting Act (FCRA).

[1.9 HR Data](#)

63. In the course of the review the EDPB review team was approached by the DoC to further discuss this issue. The main topic was the possible loss of European oversight for European employees and their expectation in terms of rights (notice and choice). On the other hand for certain service providers, the DoC underlined that it might be difficult to even know if they are processing employee data. Arguments and possible solutions were exchanged. The DoC took note of those and will contemplate on possible ways forward. There is no concrete outcome of the discussions yet.

[1.10 US domestic privacy update: NIST Framework](#)

64. The National Institute of Standards and Technology (NIST) presented the last version of its “Privacy Framework” (preliminary draft, 6 September 2019). The Privacy Framework, customizable by companies, aims at providing guidance to companies on how to reach a certain level of data protection (the process), without pre-setting the level to be reached (“desired privacy outcomes”).

[2 ON GOVERNMENT ACCESS TO PERSONAL DATA: RELEVANT DEVELOPMENTS IN THE U.S. LEGAL FRAMEWORK AND TRENDS](#)

65. Legal framework has not changed substantially.

[2.1 Ombudsperson mechanism](#)

66. During the review, Keith Krach presented himself as the new Under Secretary for Economic Growth, Energy, and the Environment of the U.S. Department of State, and the Privacy Shield Ombudsperson. He stressed that the Ombudsperson mechanism needs to provide an effective, empowered channel of review for EU individuals.
67. He also confirmed to be independent from the Intelligence Community (IC), and stressed, as his predecessors did during the first and second reviews, that he will not sign his name to a letter if he would have any remaining doubts on the completion of appropriate redress.
68. The Ombudsperson’s staff then reported that the only request received under the Ombudsperson mechanism was in agreement with the EU Centralized Body found to be deficient.

69. Referring to a hypothetical case, the staff then presented in general terms the procedures and powers of the Ombudsperson, stressing that the Ombudsperson would have access to all information he needs to perform its duties and that all incidents of non-compliance would have to be remedied, including the purging of data. It was also provided that violations of section 702 FISA would be reported to the FISA Court.
70. No further specific information about how the Ombudsperson would cooperate with the IC were shared, as the Ombudsperson reported that those procedures continue to be classified.

2.2 Inspector General (IG)

71. The Inspector General of the IC gave an overview of how IGs are set up and operate within the U.S. government and the U.S. legal system. He stressed that IG's are independent from the bodies they oversee, and that they are empowered by law to review and investigate any abuse of power.
72. The IG reported that the request which was made under the Ombudsperson mechanism (and found to be deficient) was also examined by the office of the IG.
73. The IG confirmed that the office could take up any hint of an abuse of power, also on its own initiative. However, the IG only investigates concrete cases and does not review policy.
74. During the last year, the IG office has not investigated any matter related to the Privacy Shield.
75. Questioned about how the office of the IG would handle an Ombudsperson request, the IG explained that it would depend on the case, but that he may refer to an agency, and that a remedy may be proposed to the ODNI. He added that Congress would also be informed about recommendations and about cases where the recommendation is not followed through.
76. Further, the IG explained that the Ombudsperson would also be informed of the findings and recommendations to the ODNI necessary for the Ombudsperson to perform his duties. In order to protect sources and other sensitive information, in the report to the Ombudsperson, the IG may remove information from the report to the ODNI. As a consequence, the information shared with the Ombudsperson may not necessarily be identical to the information shared with the ODNI.
77. Finally, the IG clarified that his resources are not decided upon by the Government, but by Congress.

2.3 PCLOB

78. The summer before the third annual review, the Senate confirmed the last two members of the PCLOB. The Chair of the PCLOB underlined that the PCLOB is thus now fully staffed for the first time since 2016.
79. The staff has also doubled since the last review, and 7 new projects have been launched. Overall, the PCLOB is now working on 10 projects and also strengthened its knowledge in terms of technology.
80. For the first time, the PCLOB released an agenda of their current projects, which it will update every six months. The PCLOB also published strategic goals for the next three years, among them technology is identified to be the key factor for privacy.
81. The PCLOB representatives recalled the history of the agency and its functioning.
82. Regarding the current projects, the Chair underlined that the Board is currently working on the following issues:
 - Regarding NSA's collection of detailed call records under the USA Freedom Act. The report is expected to be finalized later this year.

- Regarding facial recognition in airports, work has started recently.
 - Regarding the terrorist watchlist, a project is ongoing as well, yet without any forecast date. It was however underlined that the mere fact of working on a subject already sends a signal.
 - Regarding EO 12 333, work is still ongoing:
 - a. 3 deep-dive reviews were organized on this subject, 2 of those related to the CIA (1 of them is finalized and transmitted to the Congress), 1 to the NSA (on XKeyscore).
 - b. The PCLOB is also providing advice on a range of guidelines on EO 12 333 for internal use.
 - c. The PCLOB Chair indicated that they hope some work will be completed and made available in a relative near future.
83. Regarding the calendar of work concerning EO 12 333, the Chair indicated that each deep-dive review can be finalized independently from the others, and be declassified separately. However, the Chair of the PCLOB underlined that in spite of their strong policy towards the broadest dissemination of their works, it was unlikely that these reports would ever be (fully) declassified.
84. Regarding Section 215 and whether their report will be issued by the end this year, the Chair of the PCLOB confirmed that they hope to deliver it in sufficient time, so that it will be available to the Congress in the context of the possible re-authorization of this section.
85. When questioned on whether the PCLOB's report on Section 702 could and would be updated, the Chair of the PCLOB indicated that FBI's access and use of the data would partially be reviewed, but that the PCLOB did not intend to update the whole report.
86. Regarding the mandates the PCLOB gives itself and its work program, the Chair of the PCLOB indicated that the PCLOB has a holistic approach and that its reports focus on collection, but also look at storage, use of data, compliance mechanisms, as well as sharing and dissemination. It was also underlined that the PCLOB's focus evolves where the practice goes, and needs to migrate to those, even when they are not yet known to the public.
- 2.4 ODNI and Department of Justice presentation and Q/A on government access to personal data: relevant developments in the U.S. legal framework and trends**
87. The Chief Privacy Officer of the ODNI confirmed again that the function of his office was to advise on the policies regarding civil liberties and privacy, according to the statutes, and that the officers also have the power to conduct investigations, which includes to have access to all the materials and records needed.
88. When performing their missions, they are bound by statutes which govern their actions, by Executive orders, Attorney general's guidelines, Presidential Directives, and orders of courts. This office also provides the public with new interpretations issued by the FISC (either along with the decision or with a summary if the decision itself cannot be provided).
89. The Chief Privacy Officer of the ODNI reported that no major changes took place since the last review. He confirmed that PPD 28 remains in full force and effect.
90. In this regard, he underlined that PPD 28 demonstrates a strong preference to conduct targeted surveillance (as tailored as feasible) rather than bulk, which is, in principle, allowed only for six purposes.

91. He reaffirmed that bulk collection is neither generalised, nor mass collection, and that “bulk collection” is usually a choice, for instance to identify a target.
92. In view of a question raised by the CJEU during the hearing on the Schrems II case, in particular on footnote 5 of PPD 28, after extensive and detailed exchanges, the following elements were clarified:
 - This footnote is not applicable to Section 702 as it is not a bulk collection program (since it is based on the use of selectors). Nevertheless, sections 1, 3 and 4 of PPD 28 apply.
 - This footnote applies to EO 12 333, for instance.
 - This footnote would mean that in addition to the six purposes foreseen under PPD 28 for bulk collection, PPD 28 allows (through this footnote) an additional situation where bulk collection can take place: when bulk collection is temporary, in order to identify a target. In this case, it appears to be possible to derogate from the six other purposes foreseen under PPD 28 to undertake a bulk collection of data, but only temporarily, for another authorized purpose of collection, and in this case, Section 1 of PPD 28 would still apply.
 - Questioned on what “temporary” would mean, the answer was not very clear. It seems that, as soon as the collected data has been processed to help identify the target, useless data is no longer useful is deleted.
93. Concerning targets and selectors under Section 702, the Chief Privacy Officer of the ODNI recalled that the distinction between a selector and a target is important: the target should be a “person”, while a “selector” is any communication identifier (e.g., email address, phone number, etc.) allowing to isolate the person’s communication data from the bulk. However, questioned on whether a person should necessarily be only one single individual, he acknowledged that in some cases a person could be a group comprising more than one individual (e.g., the users of an email account), provided the size of the group remains limited and that any member of the group needs to have a link with the foreign intelligence at stake and to be a non-US person.
94. The way a person is selected is through the tasking of a selector, which is documented both for approval and oversight.
95. It was stressed that each selector has to be an account used by a person and that it cannot be the name of a person. It has to be a communication account identifier, thus communication always has to be from or to the selector. It was also confirmed that these safeguards related to the tasking of selectors only apply within the framework of Section 702.
96. Questioned on the time limit for which a selector is tasked, it was underlined that a selector is tasked “for as long as it brings back foreign intelligence”. Regular checks would thus be performed to confirm that is still useful and necessary.
97. As regards to PRISM and UPSTREAM collection and the filtering of communications, no additional information was presented during this review.
98. At the time of targeting, the NSA shall provide a written explanation to allow for an *ex ante* review in the IC before tasking the selector, as well as a post review by the DoJ. It was recalled that in case of an acknowledged incident, collection stops, the underlying information has to be purged, and, if any reports were based on that information, these reports must be recalled (this is a standard procedure for reports in this domain).

99. In case of an incident, the office of the Privacy Officer would also have to look at the context in which it occurred and to report non-compliance to the FISC (in the context of section 702), with a description of the scope of the incident and of reasons why it happened. The Court then would follow-up on these reports, for instance by determining, in the annual certification process, whether those compliance incidents effectively rendered certification inadequate. It could also issue a deficiency order to have it remedied within 30 days. In addition, quarterly reports on incidents are also sent to the FISC.
100. In addition, the Chief Privacy Officer of the ODNI stressed that semi-annual reports of compliance incidents for the Congress are declassified to the extent allowed and made available on IC on the record, by the DoJ. These reports also show the trends of non-compliance and comments, which provide more useful information than the statistics (see the last one of March 2019).
101. Brief updates were also provided on cases introduced or ruled since the last review concerning FISA §1806 (two cases of the 9th Circuit - Jewel and Fazaga), as well as FOIA (ACLU v. NSA before the appellate court and the following cases, as well as Food marketing Institute v. Argus Leader Media from the Supreme Court).
102. Concerning the Wikimedia case, the DoJ stressed that the first instance considered that the complainants lacked standing, but this judgement was overturned by the appellate court. The case is still pending, while another case was ruled and dismissed on substance, but is being appealed too.
103. Concerning Section 501, for which the Administration is seeking reauthorization of this authority, it was recalled that the NSA is not using it any longer, because the information were too narrow and thus not sufficiently useful.
104. Questioned on how the additional safeguards afforded to the data of EU residents transferred to the US through the Privacy Shield would be reflected in executive agreements concluded between the US and another third country in the context of the Cloud Act, the DOJ indicated that it could not answer this question yet.

LIST OF ABBREVIATIONS

DoC: Department of Commerce

FTC: Federal Trade Commission

IG: Inspector General

APA: Administrative Procedure Act

FISA: Foreign Intelligence Surveillance Act

FISC: Foreign Intelligence Surveillance Court

PCLOB: Privacy and Civil Liberties Oversight Board

PPD-28: Presidential Policy Directive n°28

EO 12 333: Executive Order 12 333

ODNI: Office of the Director of National Intelligence

EDPB Documents



EDPB Document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal

Adopted on 28 January 2020

Table of contents

1. EDPB APPROVAL of EU-wide certification criteria (EU DP Seal): REVIEW, SUBMISSION, ADMISSIBILITY and ADOPTION	3
1.1. Submission	3
1.2. Initial admissibility of the certification criteria	4
1.3. Cooperation (informal cooperation phase at the SAs level)	4
1.4. Formal submission and approval (EDPB phase)	5
1.5. Article 64(2) opinion	6
1.6. Further steps following approval of EU Data Protection Seal	7
Workflow – EDPB’s Approval of EU Data Protection Seal Criteria of certification	8

The European Data Protection Board

Having regard to Article 42(5), Article 64(2) and Article 70(1)(o) 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 2018,¹

Having regard to Article 3 and Article 22 of its Rules of Procedure of 25 May 2018,

HAS ADOPTED THE FOLLOWING DOCUMENT

1. EDPB APPROVAL of EU-wide certification criteria (EU DP Seal): REVIEW, SUBMISSION, ADMISSIBILITY and ADOPTION

1.1. Submission

Scheme owners (which could be organisations or private companies that are not in charge of issuing certificates) or certification bodies, should formally submit their EU-wide certification criteria (in order of application):

- 1) to the competent SA (CompSA) where the scheme owners² have their headquarters;
- 2) to the CompSA where a certification body operating the certification mechanism have their headquarters³, considering the member state in which the most certificates are likely to be issued.

Furthermore, SAs can also draft certification criteria for an EU-wide certification mechanism on their own initiative⁴.

SAs can submit criteria for EU-wide certification mechanism referred to in article 42(5) for approval by EDPB pursuant to article 63 and article 70(1)(o).⁵ The SA will carry out a review to ensure that draft certification criteria meet the requirements of EU wide GDPR certification criteria, taking into account the EDPB guidelines on certification.⁶ The CompSA’s review will be aided by fully completing the

¹ References to the “EU” made throughout this document should be understood as references to “EEA”.

² A scheme owner can also be a certification body

³ The accreditation of the certification body (by either the national accreditation body (NAB) or the CompSA) also includes an assessment of the certification mechanism. In particular, it includes a check that the proposed assessment methodologies are appropriate with respect to the approved certification criteria. The accreditation will also take place where the certification body is headquartered, in accordance with the EDPB Guidelines 1/2018, paragraph 44.

⁴ The SA will act as a scheme owner.

⁵ A SA cannot submit certification criteria for an opinion if it has not already submitted its accreditation requirements for approval.

⁶ Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation

assessment template for certification criteria adopted by EDPB (both national and EU sections are required to be completed). The submission of this document to the EDPB can only be made when the CompSA considers that the criteria could be approved by EDPB (see step 3a).⁷

1.2. Initial admissibility of the certification criteria

If the draft criteria are not found acceptable by the CompSA, the CompSA will write to the scheme owner outlining the basis for its decision (see step 3b).

If the draft criteria are found acceptable by the CompSA, the CompSA will write to the scheme owner with confirmation that they will proceed to the next stage of the process and assess the draft criteria. This will trigger the following informal cooperation procedure in respect of assessing the criteria for approval.

1.3. Cooperation (informal cooperation phase at the SAs level)

The informal cooperation phase is integral in enabling an efficient Board approval procedure. The informal cooperation phase will enable the CompSA identified above to lead the assessment of the criteria and provide feedback to the scheme owner as required. The CompSA will provide timely updates to the scheme owner about all phases.

The CompSA will issue a notification updating all SAs and they will make a request seeking, on a voluntary basis, a maximum of two co-reviewers to assist with the substantive assessment of the criteria (see step 4). The request for co-reviewers is made via email to EDPB secretariat. The email communication must include the EDPB assessment template completed by the CompSA.

The informal cooperation phase (see step 4 to 6) can only start when the following documents are available in English language and can be shared with other SAs:

- the EDPB assessment template fully completed by the CompSA. It shall include information about how all relevant national legislations have been addressed and about the planned roll out in MSs; and
- a copy of the criteria for certification and any relevant annexes.

Certification criteria related to specific Member State legislation can be submitted in their national language, if available.

The role of co-reviewers will be to assist the CompSA in assessing the draft criteria. The co-reviewers should ensure that they involve experts according to the certification subject. Once the co-reviewers are confirmed, comments from them on the criteria should be provided within thirty days from the moment that the documents are shared with them. These comments will then be considered by the CompSA when carrying out its assessment. The review will mainly focus on the technical acceptability of the certification criteria (see step 5).

Following the co-review, the CompSA will circulate the draft criteria to all SAs. The EDPB Secretariat may assist with the communication among SAs (see step 6). All concerned SAs will have 30 days to respond and any significant issues could be brought to the relevant EDPB subgroup for discussion. The review will consist of making sure that national legislation has been covered appropriately and it will

⁷ See section 4.2 (paragraphs 35 – 45) of the EDPB guidelines on certification criteria.

also include the analysis of the compliance of the criteria covering the national legislation. If the SAs do not respond, the criteria will continue to the next stage of the procedure.

The CompSA can decide to repeat steps 5 & 6 as required.

Following any step of the informal cooperation phase, the CompSA can give the scheme owner the option to update the certification criteria taking into account the SAs remarks.

Following step 6 and presuming a positive outcome, the CompSA will request a subgroup session to discuss the criteria under review (see step 7). The CompSA will update the EDPB assessment template with the key points from this session. Any actions raised in the meeting can be taken forward by the CompSA and the criteria can be revised by the scheme owner.

At the end of the informal cooperation phase, the CompSA (in consultation with the scheme owner) can decide whether or not to submit the certification criteria to the EDPB for formal approval. The CompSA will make the final determination as to whether the draft criteria should be submitted to the Board for approval as per Articles 63 of the GDPR. Where the CompSA decides not to submit the certification criteria to the EDPB, the process ends (see step 8b). A resubmission of the certification criteria, at a later date, will result in a new review process.

The scheme owner should take part in the review process at the informal phase. The competent SA should inform the scheme owner of the comments made during the cooperation phase and the scheme owner should be given the opportunity to ask for clarifications and to respond⁸.

1.4. Formal submission and approval (EDPB phase)

The approval of an EU Data Protection Seal takes place under the procedure of an article 64(2) opinion.

The CompSA is asked to take into consideration the working schedule of the CEH ESG before making its submission via IMI.

The formal submission must be done via IMI platform (step 8a). It shall fulfil the following admissibility criteria for acceptance by EDPB:

- All relevant documents must be submitted in English;
- The EDPB assessment template must be completed by the CompSA and submitted (the template must be updated accordingly to the result of the initial review phase); and
- A copy of the certification criteria and any annexes must be submitted.

The secretariat will check that all documents are present and complete. The secretariat may request the CompSA to provide, within a specific timeframe, with additional information needed for the file to be complete. As a general rule, and without prejudice to other translations where necessary or required by law, all relevant documents should be provided by the applicant in the language of the CompSA and also in English. When necessary, for instance documents not originating or drafted by the SA, the documents submitted by the CompSA will be translated into English by the secretariat without undue delay. In such cases, when the competent authority agrees on the translation, and the

⁸ The competent SA has to ensure that the scheme owner is informed about this possibility and is given such opportunity.

Chair and the CompSA decide that the file is completed, the secretariat, on behalf of the Chair, will circulate the file to the members of the Board.

The opinion of the Board shall be adopted within eight weeks after the Chair and the CompSA (where relevant) have decided that the file is complete. It may be extended by a further six weeks, taking into account the complexity of the subject matter, upon decision of the Chair on its own initiative or at the request of at least one third of the members of the Board.

Before draft opinions are submitted to the vote of the Board, they shall be prepared and drafted by the secretariat and, upon decision of the Chair, together with a rapporteur and expert subgroups members. Depending on the scope of the certification mechanism, expertise of other EDPB subgroups may be requested in order to prepare the opinions.

Upon decision of the chair, a drafting team can be set up, depending on the timing of submission, via email or at a CEH meeting. The call for the drafting team volunteers will be made by the Secretariat together with CEH experts group co-ordinators. In order to avoid conflicts of interest, the CompSA should not be part of the core drafting team. However, any questions can always be addressed by the core drafting team to the CompSA.

The secretariat and the drafting team (where relevant) review the submitted criteria for certification and supporting documents (including the assessment template) and draft the opinion. This will always involve consideration of what was stated in previous opinions on the same subject, in order to ensure consistency. The EDPB assessment template submitted by the CompSA can be used as an internal working document when preparing the draft opinion. This review must take place within the opinion deadlines.

1.5. Article 64(2) opinion

Under article 64(2) and 70(1)(o), EDPB shall issue an opinion and approval pertaining to matters outlined in Article 42(5) of the GDPR (see step 9).⁹

The rules of article 10 of the EDPB rules of procedure apply for the adoption of an opinion¹⁰. The SA who decides to ask for an Opinion under article 64(2) will have to provide written reasoning for the request, as per article 10(3) RoP. In the context of a request for approval by EDPB of an European Data Protection Seal for criteria of certification, the CompSA has to ask for an Opinion under article 64(2) regarding a matter producing effects in more than one member states.

EDPB's approval process is completed by the approval or by the rejection of the EU data protection seal request for the submitted criteria. Under article 64(2) there is no need for a follow-up of the opinion of the Board.

⁹ Article 64(2) GDPR allows the SAs to request an Opinion regarding a matter of general application or producing effects in more than one member states. Since the EU DP Seal has EU-wide effects, the Opinion of the Board falls within the scope of article 64(2), rather than article 64(1).

¹⁰ It should also be noted that only 'approve' or 'reject' opinions are possible as it could be misleading to 'approve' a seal with remaining issues to handle.

EDPB's opinion under article 64(2) is applicable in all Member States.¹¹

1.6. Further steps following approval of EU Data Protection Seal

The following steps must be completed after the approval of EU DP Seal criteria:

- the Secretariat publishes the opinion containing the EDPB data protection seal approval or rejection;
- the CompSA will inform the scheme owner about the outcome of EDPB's approval process for the EU Data Protection Seal request.;
- the lead/co-ordinating CompSA is responsible for ensuring the transmission to the Secretariat of the required documents for the publication in the EDPB public register.

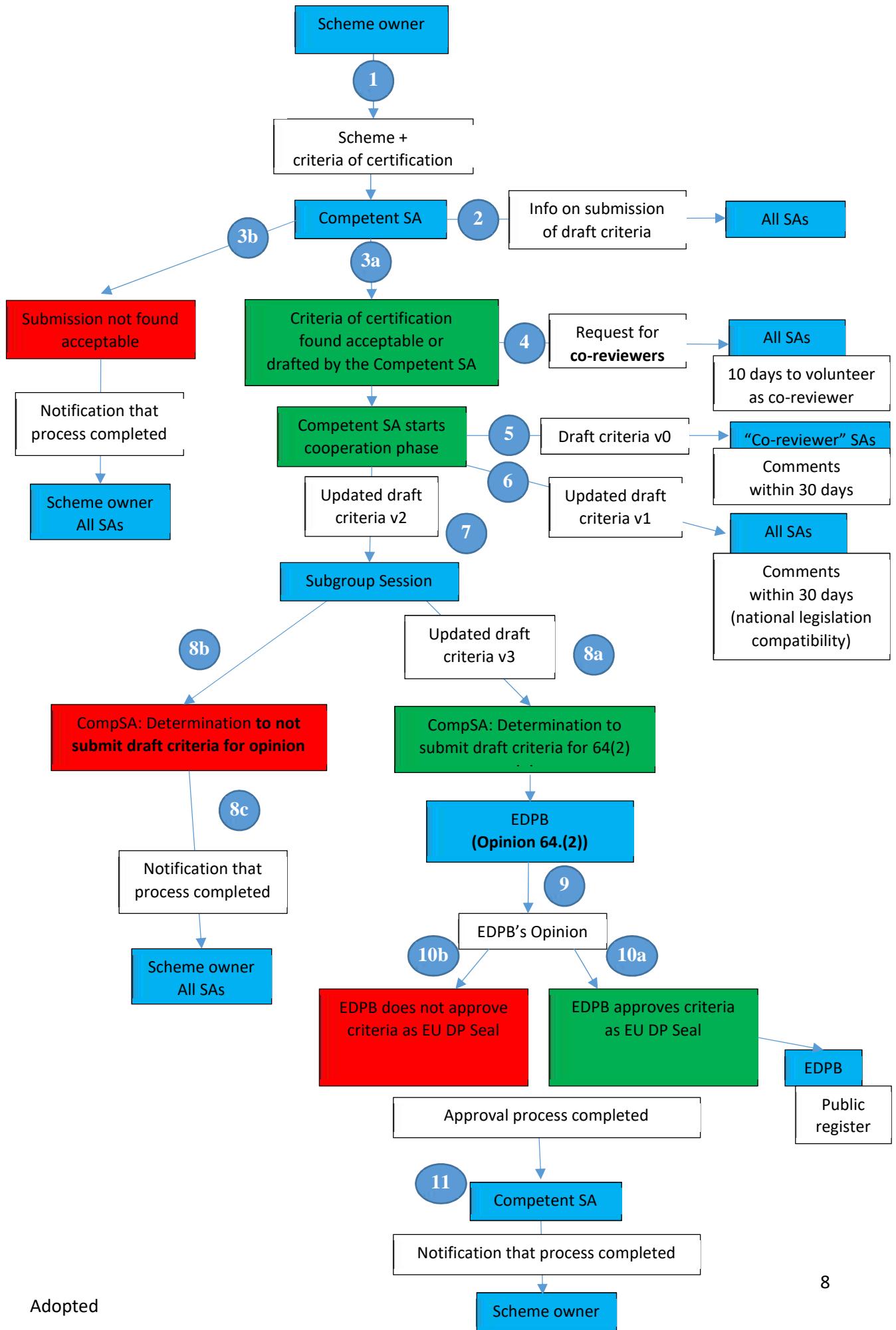
If EDPB rejects the EU data protection seal request via a negative opinion:

- the CompSA informs the scheme owner that, according to the EDPB's opinion, the certification mechanism does not meet the requirements for EDPB approval.
- the CompSA can decide to resubmit certification criteria for requesting an EU data protection seal. The CompSA can decide either to start a new informal cooperation phase or submit the criteria directly to the article 64(2) opinion phase.

Guidance on the European Commission's powers under Article 43(8) and (9) will be added in due course, along with any further requirements for international transfer criteria.

¹¹ If an SA does not follow the opinion issued and does not accept the EU data protection seal approval, any other SA or the Commission could raise the matter to the board in order to get a binding decision under article 65(1)(c)¹¹.

Workflow – EDPB's Approval of EU Data Protection Seal Criteria of certification



**Joint EDPB-EDPS contribution to the public consultation on
the draft template relating to the description of consumer
profiling techniques (Art.15 DMA)**

Adopted on 20 September 2023

EDPB-EDPS COMMENTS ON THE DRAFT TEMPLATE RELATING TO THE AUDITED DESCRIPTION OF CONSUMER PROFILING TECHNIQUES PURSUANT TO ARTICLE 15 OF THE DIGITAL MARKETS ACT ('DMA')

1. INTRODUCTION

On 31 July 2023, the European Commission launched a Public Consultation¹ concerning the template for the description of consumer profiling techniques and audit of such reports that designated gatekeepers will have to submit annually under Article 15 of the Digital Markets Act² ('DMA').

By letter of 31 July 2023, the Commission invited the European Data Protection Board ('EDPB') and the European Data Protection Supervisor ('EDPS') to provide feedback to the template. The EDPB and the EDPS welcome the opportunity to provide comments on the draft template.

In addition, as member of the DMA High Level Group under Article 40 of the DMA, both the EDPB and the EDPS remain available in that quality and beyond to advise the European Commission, with a view to ensuring regulatory consistency, or to provide advice for any matter of general implementation or enforcement of the DMA when data protection issues are at stake³.

2. GENERAL COMMENTS

The EDPB and EDPS recall that gatekeepers shall submit to the Commission, within 6 months after their designation, the independently audited descriptions of any techniques for profiling of consumers that they apply to or across their core platform services. The European Commission shall then transmit that audited description to the EDPB, pursuant to Article 15(1) DMA.

In accordance with Article 36 DMA, the information collected pursuant to Article 15 shall also be used for the purposes of Regulation (EU) 2016/679⁴ ('GDPR'). Recital (72) DMA clarifies that the independently audited descriptions may be relied upon to inform the enforcement of Union data protection rules.

The objectives of Article 15 DMA, as set out in Recital 72, include enhancing transparency and accountability regarding gatekeeper's profiling techniques as well as facilitating fairness and contestability of their respective core platform services. Such transparency should among others "help avoiding that deep consumer profiling will become the *de facto* industry standard and allow competitors to differentiate themselves through the use of superior privacy guarantees"⁵.

¹ https://digital-markets-act.ec.europa.eu/consultations/consultation-template-relating-reporting-consumer-profiling-techniques_en.

² Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1–66.

³ Article 40(5) DMA.

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

⁵ https://digital-markets-act.ec.europa.eu/consultations/consultation-template-relating-reporting-consumer-profiling-techniques_en. In the same vein, recital (72) of the DMA indicates that "*transparency puts external*

Transparency about gatekeepers' profiling techniques should bring to light how gatekeepers comply with data protection law. To be effective, the audited description of profiling techniques should provide supervisory authorities with sufficient insights to inform the enforcement of Union data protection rules in a meaningful manner. Even though the DMA does not have the force of *lex specialis* in relation to the GDPR or the ePrivacy Directive⁶, it is clear that Article 15 DMA will only be effective in providing transparency and accountability if the information gatekeepers are expected to share with the Commission is sufficiently comprehensive.

As a preliminary remark, the EDPB and the EDPS note that under Article 15(1) DMA the audited description should cover profiling techniques that gatekeepers apply 'to or across' their core platform services. In this regard, the EDPB and the EDPS recommend that the introduction to the template clarifies whether the Commission expects to receive different audited descriptions of profiling techniques for each of the core platform services of the gatekeeper, or whether a single description of profiling techniques for all concerned core platform services would be more appropriate. The EDPB and EDPS consider that if different core platform services of the gatekeeper use the same profiling techniques, one audited description could be submitted, provided that the audit of the description encompasses all core platform services concerned. Otherwise, multiple descriptions should be provided.

The EDPB-EDPS comments focus primarily on Section 2 of the draft template ('Information about the profiling techniques of consumers').

Without prejudice to the comments formulated below on Sections 3 to 5 of the template, the EDPB and the EDPS consider that the template should not serve as a replacement for the implementing act which the Commission may adopt pursuant to Articles 15(2) and 46(1)(g) DMA to develop the methodology and procedure of the audit. In particular, the EDPB and the EDPS are concerned that the template alone would not provide sufficient safeguards against low quality or otherwise unreliable audits on behalf of gatekeepers. Even if information obtained from gatekeepers (e.g., in the context of Sections 3 to 5 of the template) could inform the preparation of such an implementing act, the EDPB and the EDPS consider that a detailed methodology and procedure for the audited description of profiling techniques should be set out separately. This would ensure that gatekeepers would follow the correct and Commission-vetted process to collect and convey the information on consumer profiling sought by the Commission.

The information that the Commission obtains via the audited descriptions under Article 15 will in first instance serve as input for the European Commission to carry out its tasks under the DMA and is without prejudice to the tasks and powers of supervisory authorities under the GDPR. As a consequence, the EDPB and the EDPS underline that any tacit or explicit approval or expression of the

pressure on gatekeepers not to make deep consumer profiling the industry standard, given that potential entrants or start-ups cannot access data to the same extent and depth, and at a similar scale. Enhanced transparency should allow other undertakings providing core platform services to differentiate themselves better through the use of superior privacy guarantees."

⁶ Article 8(1) DMA states that (emphasis added) "*The gatekeeper shall ensure and demonstrate compliance with the obligations laid down in Articles 5, 6 and 7 of this Regulation. The measures implemented by the gatekeeper to ensure compliance with those Articles shall be effective in achieving the objectives of this Regulation and of the relevant obligations. The gatekeeper shall ensure that the implementation of those measures complies with applicable law, in particular Regulation (EU) 2016/679, Directive 2002/58/EC, legislation on cyber security, consumer protection, product safety, as well as with the accessibility requirements.*" Recital (12) DMA adds that the Regulation applies "*without prejudice to the rules resulting from other acts of Union law regulating certain aspects of the provision of services covered by this Regulation, in particular Regulations (EU) 2016/679 (...) and Directives 2002/58/EC (...), as well as national rules aimed at enforcing or implementing those Union legal acts.*"

European Commission on how a gatekeeper processes personal data for consumer profiling or how it informs consumer about profiling techniques does not automatically entail that the gatekeeper is complying with the GDPR, which is for supervisory authorities to verify⁷.

In addition, the information requested or shared under Article 15(1) DMA is without prejudice to the powers and competences of the Commission and supervisory authorities to request gatekeepers for access to additional information in the exercise of their respective investigative powers and enforcement⁸.

3. COMMENTS TO SECTION 1 OF THE TEMPLATE

The EDPB and EDPS note that the stated objective of Section 1, according to the introduction of the template, is to allow the Commission to obtain “*information on the identity of the gatekeeper*”. The EDPB and the EDPS therefore recommend replacing the current title of Section 1 (“*General information on profiling description*”) with “**Information on the identity and corporate structure of the gatekeeper**”.

Concerning 1.2 ‘Please provide the name of each member of your organisation or external expert which contributed to the drafting of the submitted description of the consumer profiling techniques’

The EDPB and the EDPS note that it would be important for gatekeepers to not only provide the Commission with the name of each person involved in the drafting of the submitted description of the consumer profiling techniques, but also with information about the function and role of such persons. That information could allow the Commission to detect or further investigate potential conflicts of interest or duties among persons who contributed to the drafting of the audited description.

In addition, the EDPB and the EDPS consider it unclear what it means to ‘contribute to the drafting’ of the audited description, and that this could be narrowly interpreted by gatekeepers. It appears important to have a complete overview of all relevant persons involved in the preparation of the audited description⁹. For example, it would appear appropriate for technical or legal experts that provided reports on the functioning of automated systems used for consumer profiling - which ultimately serve as input to the description of the techniques - to be mentioned.

The EDPB and the EDPS recommend redrafting point 1.2. of Section 1 of the template as follows:

‘Please provide the name, **function and role of each member of your organisation or external expert which contributed to the ~~drafting of~~ submitted description of the consumer profiling techniques’**

⁷ Article 8(3) of the Charter of Fundamental Rights of the European Union (2000/C 364/01).

⁸ See Article 23(1) and (2) DMA and Article 58(1) GDPR.

⁹ For the sake of completeness, the EDPB and EDPS consider that individual contributors should not be mentioned in the publicly available overview of the audited description, as referred to in Article 15(3) DMA.

4. COMMENTS TO SECTION 2.1. OF THE TEMPLATE

Concerning a) ‘the specific purpose(s) pursued by the profiling technique(s) and for which they are used’

As a preliminary remark, the EDPB and the EDPS wish to underline that information about the profiling purposes should not consist of a generic reference to the evaluation of personal aspects to analyse or predict aspects concerning consumers¹⁰. The information about the specific purposes pursued by the profiling techniques and for which they are used should focus on the final results or outcomes which are expected or obtained by the gatekeeper from the profiling process (e.g., predicting the near future consumer purchasing needs or behaviour to tailor advertising messages or prices to their individual situation)¹¹. In this regard, the EDPB and the EDPS also note that recital (72) DMA refers to “*the purpose for which the profile is prepared and eventually used*”.

Against this background, the EDPB and the EDPS welcome that point a) of Section 2.1. of the template refers to the *specific* purposes pursued by the profiling techniques and recommend including an explanatory footnote with a few negative and positive examples of purpose descriptions to guide gatekeepers when compiling and sharing the information requested¹².

Concerning b) ‘the legal ground relied on by the gatekeeper under Article 6(1) of Regulation (EU) 2016/679 and whether consent is required under points a) to d) of Article 5(2) of Regulation (EU) 2022/1925 for each purpose of profiling consumers’

In accordance with the accountability principle, it is the task of gatekeepers, when acting as controllers in relation to consumer profiling, to demonstrate how they comply with the data protection principles outlined in Article 5(1) GDPR¹³. This includes the lawfulness principle¹⁴ and the associated requirement of securing an appropriate legal basis for processing personal data¹⁵.

The EDPB and the EDPS recall that gatekeepers may also need to be able to demonstrate that an exception to the prohibition to process special categories of personal data under Article 9(2) of the GDPR applies in the context of their consumer profiling processing activities. In some instances, processing of personal data and special categories of data may also be subject to further limitations¹⁶,

¹⁰ Article 4(4) GDPR.

¹¹ [Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 \(WP251rev.01\)](#), As last Revised and Adopted on 6 February 2018, page 7: “*profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse or make predictions about individuals [e.g., regarding their ability to perform a task, interests and likely future behaviour]. The use of the word ‘evaluating’ suggests that profiling involves some form of assessment or judgement about a person. A simple classification of individuals based on known characteristics such as their age, sex, and height does not necessarily lead to profiling. This will depend on the purpose of the classification. For instance, a business may wish to classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its clients without making any predictions or drawing any conclusion about an individual. In this case, the purpose is not assessing individual characteristics and is therefore not profiling.”*

¹² Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation (WP 203), Adopted on 2 April 2013, page 16: “*a purpose that is vague or general, such as for instance ‘improving users’ experience’, ‘marketing purposes’, ‘IT-security purposes’ or ‘future research’ will - without more detail - usually not meet the criteria of being ‘specific’.*”

¹³ Article 5(2) GDPR.

¹⁴ Article 5(1)(a) GDPR.

¹⁵ Article 6(1) GDPR.

¹⁶ The EDPB and the EDPS also note that limitations to the processing of data may also stem from Directive

such as when it qualifies as automated decision-making under Article 22(1) GDPR¹⁷, or when it is used by gatekeepers who qualify as a provider of an online platform under the Digital Services Act ('DSA') to present advertisements to recipients of the service¹⁸.

Lastly, in relation to Article 5(2) of the DMA, in case the gatekeeper believes that the processing does not require consent and can rely on an alternative and permissible lawful ground under Article 6(1) GDPR, the gatekeeper should be required to demonstrate why it is appropriate to rely on Articles 6(1)(c), (d) or (e) GDPR. In this respect, account should be taken of the limitations on gatekeepers' ability to rely on Article 6(1)(d) or (e) GDPR to process consumer data, in light of their type of activity and their essentially economic and commercial nature¹⁹.

In light of the above, the EDPB and the EDPS recommend redrafting point b) of Section 2.1. of the template as follows:

'the legal basis relied on by the gatekeeper under Article 6(1) of Regulation (EU) 2016/679 for the processing referred to in point g) of the template, and, if applicable, the exception under Article 9(2) and/or Article 22(2) and (4) of Regulation (EU) 2016/679 that the gatekeeper relies upon, together with a justification for reliance on such legal basis and exception; and whether consent is required under points a) to d) of Article 5(2) of Regulation (EU) 2022/1925 for each purpose of profiling consumers and, if consent is not required, why it is appropriate to rely on Articles 6(1)(c), (d) or (e) of Regulation (EU) 2016/679'

In addition, the EDPB and the EDPS recommend adding a new point to the list below point b), considering that certain gatekeepers might seek to rely on the legitimate interests lawful ground under Article 6(1)(f) GDPR when carrying out consumer profiling in their core platform services, in particular in cases falling outside of the scope of Article 5(2) DMA. In that context, the EDPB and the EDPS would consider it necessary to ask gatekeepers to share with the Commission relevant information necessary to assess the lawfulness of the gatekeeper's reliance on that lawful ground, including: (i) a summary of the legitimate interest balancing test they have carried out in accordance with Article 6(1)(f) GDPR²⁰; (ii) a description of the mechanisms they made available to consumers to

2002/58/EC (the 'ePrivacy Directive'), which contains specific requirements in relation to storing information, or accessing information in the terminal equipment of a consumer, as well as additional requirements which would apply to providers of number-independent interpersonal communications services qualifying as gatekeepers and seeking to use certain types of information in the context of their consumer profiling techniques.

¹⁷ Article 22(2) GDPR sets out three exhaustive cases in which the prohibition under Article 22(1) GDPR on specific types of automated decision-making would not apply, notably when the decision: is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent. See also Article 22(4) GDPR: "Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

¹⁸ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102, Article 26(3).

¹⁹ Judgment of the Court of Justice of 4 July 2023 *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21 ECLI:EU:C:2023:537, paragraphs 133 and 137.

²⁰ The summary of the balancing test should include information on (i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed, (ii) the need to process personal data for the purposes of the legitimate interests pursued, and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence. See the [EDPB Guidelines 8/2020 on the targeting of social media users](#), Version 2.0, adopted on 13 April 2021, para. 50, with reference to Judgment of the Court of Justice of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, para. 95.

object to such profiling under Article 21 GDPR; (iii) how objection requests are honoured in practice; and (iv) any compelling legitimate grounds for continuing the processing despite objection requests.

Concerning c) ‘a numbered list with a detailed description of each category of personal data and data derived from user activity (in particular, distinguish data and personal data categories actively provided by consumers²¹ from observed data²²) and sources for each of these categories of data and personal data processed for profiling consumers applied to or across the designated core platform services (in particular, distinguish data and personal data originating from the gatekeeper’s services, including core platform services, from data and personal data originating from third parties’

As a baseline for clarifying the scope of the information requested, the EDPB and EDPS would like to underline the distinction between personal data that is ‘provided’ by the data subject and personal data that is created by the data controller on the basis of the former (i.e., ‘derived’ or ‘inferred’ data). The EDPB has had the opportunity to elaborate on the distinction between those categories of data in its guidelines on Article 20 of the GDPR²³ and on the targeting of social media users²⁴.

In light of this distinction, the examples provided of data ‘derived’ from user activity in point c) of Section 2.1. of the template, as well as other references in its wording and its explanatory footnotes, may be misunderstood by gatekeepers. Indeed, the EDPB and the EDPS understand Recital 72 DMA as referring to all types of data which are derived from user activity (in the broad sense), including not only ‘provided’ and ‘observed’ data, but also ‘derived’ or ‘inferred’ data.

When listing the sources for the categories of personal data processed for profiling consumers, the EDPB and the EDPS recommend that gatekeepers are required to provide the Commission not only with information on “data originating from third parties” as such, but also data resulting from the “use of third party services”.

²¹ “For example, profile information (e.g. age, sex, location and other) provided by consumers through any core platform service, or provided through any other service of gatekeeper, when this data is combined or cross-used with that of a core platform service.”

²² “Observed data are understood as data provided by the consumer by virtue of using a service or device. For example, data related to, or derived from, the activity of the consumer on the gatekeeper’s core platform services or other services (e.g. the content that a user has consulted, shared or liked) as well as data related to, or derived from, the use of devices on which the gatekeepers’ core platform services or services are provided (e.g. GPS location).”

²³ [Article 29 Data Protection Working Party Guidelines on the right to data portability \(WP 242 rev.01\)](#), as last revised and adopted on 5 April 2017, pages 10 and 11: “In general, given the policy objectives of the right to data portability, the term “provided by the data subject” must be interpreted broadly, and should exclude “inferred data” and “derived data”, which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include all other personal data provided by the data subject through technical means provided by the controller. Thus, the term “provided by” includes personal data that relate to the data subject activity or result from the observation of an individual’s behaviour, but does not include data resulting from subsequent analysis of that behaviour. By contrast, any personal data which have been created by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.”

²⁴ EDPB Guidelines 8/2020 on the targeting of social media users Version 2.0, Adopted on 13 April 2021, pages 13 and 14: ““Provided data” refers to information actively provided by the data subject to the social media provider and/or the targeter. (...) Observed data are data provided by the data subject by virtue of using a service or device. (...) – “Inferred data” or “derived data” are created by the data controller on the basis of the data provided by the data subject or as observed by the controller.”

Therefore, the EDPB and the EDPS recommend redrafting point c) of Section 2.1. of the template as follows:

*'a numbered list with a detailed description of each category of personal data and data derived from user activity (in-particular, distinguish data and personal data categories actively provided by consumers from observed data **and from derived or inferred data**) and sources for each of these categories of data and personal data processed for profiling consumers applied to or across the designated core platform services (in particular, distinguish data and personal data originating from the gatekeeper's services, including core platform services, from data and personal data originating from third parties **and/or the use of services of third parties**)'*

Concerning d) 'a detailed description of the inferred data²⁵ about consumers from the processing of the data and personal data listed in point c)'

In line with the observations and recommendations concerning point c) above, the EDPB and the EDPS recommend clarifying that gatekeepers should report on data that they derive or infer from the processing of the data covered by point c) of Section 2.1.

Therefore, the EDPB and the EDPS recommend redrafting point d) of Section 2.1. of the template as follows:

*'a detailed description of the **derived or inferred data** about consumers from the processing of the data and personal data listed in point c), **as well as an explanation of how such derived or inferred data were created'***

Additionally, the EDPB and the EDPS recommend aligning the first sentence of the explanatory footnote in point d) - referring to the definition of 'inferred data' - with the EDPB guidelines on the targeting of social media users, as follows: '*Inferred data are understood as data **created** by the gatekeeper from the processing of observed data **and/or from** data actively provided by consumer*'.

Concerning e) 'the retention duration of each category of data and personal data listed in points c) and d) and of the profiling itself'

The EDPB and the EDPS welcome point e) of Section 2.1. of the template, which would provide information relevant to assessing compliance with the principle of storage limitation²⁶.

Nonetheless, the EDPB and the EDPS recall that Recital (72) states that the audited description of gatekeepers' consumer profiling techniques should concern "*the duration of the profiling*" which has a broader scope than the reference to personal data storage periods. The EDPB and the EDPS consider that information about the "duration of the profiling" should unambiguously indicate the time during which the consumer profiling process occurs - from the moment when gatekeepers collect data until the moment they apply a profile to the individual²⁷. In addition, the EDPB and EDPS consider that gatekeepers should be requested to justify the chosen duration.

Therefore, the EDPB and the EDPS recommend redrafting point e) of Section 2.1. of the template as

²⁵ *"Inferred data are understood as data derived by the gatekeeper from the processing of observed data or data actively provided by consumer. For example, consumers' interests or socio-economic status. Further guidance on the distinction between provided data, observed data and inferred data, can be found in the European Data Protection Board's [Guidelines on the targeting of social media users](#)."*

²⁶ Article 5(1)(e) GDPR.

²⁷ [Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 \(WP251rev.01\)](#), as last Revised and Adopted on 6 February 2018, page 12.

follows:

'the duration of the profiling process, as well as the retention duration of each category of data and personal data listed in points c) and d), accompanied by a justification of the chosen duration and of the profiling itself'

Concerning f) 'a numbered list with a detailed description of the technical safeguards in place to avoid the presentation of advertisements on the gatekeeper's interface based on profiling of minors or children, including a description of how user data is collected, used or processed in a way that allows the gatekeeper to identify a user as a minor, as well as quantitative indicators to measure the successful identification of minors'

The EDPB and the EDPS take note that gatekeepers that qualify as online platforms under the DSA are prohibited from presenting advertisements based on profiling to minors under Article 28(2) of the DSA. The EDPB and the EDPS further note that gatekeepers qualifying as online platforms are also prohibited from presenting advertisements based on profiling using special categories of personal data under Article 26(4) of the DSA. At the same time, the data protection and privacy interests of end users may be significantly affected even where the profiling practices of gatekeepers do not result in the presentation of advertisements to minors or are based on profiling using special categories of data.

The EDPB and the EDPS recommend the Commission to inquire more generally about the technical safeguards that gatekeepers have in place to protect the rights and freedoms of end users when displaying advertisements on the basis of profiling, including (but not limited to) situations where end users are minors or otherwise vulnerable, and where there is a possibility that the presentation of advertising would be based on profiling using of special categories of personal data.

In addition, Article 28(3) of the DSA states that, when complying with the prohibition under Article 28(2) of the DSA, online platforms are not obliged to process additional personal data in order to assess whether the recipient of the service is a minor. Thus, the EDPB and the EDPS recommend clarifying in a footnote that the information sought by the Commission under point f) of Section 2.1. of the template should not be read as obliging gatekeepers to process additional personal data in order to assess whether the recipient of the service is a minor.

In light of the above considerations, the EDPB and the EDPS recommend redrafting point f) of Section 2.1. of the template as follows:

'a numbered list with a detailed description of the technical safeguards in place to protect the rights and freedoms of end users when displaying advertisements on the basis of profiling, and, if applicable including measures to avoid the presentation of advertisements on the gatekeeper's interface based on profiling of minors or children to minors or profiling based on special categories personal data referred to in Article 9(1) of Regulation (EU) 2016/679; including this shall include a description of how user data is collected, used or processed in a way that allows the gatekeeper to identify a user as a minor, as well as quantitative indicators to measure the successful identification of minors, if applicable, and a description of whether (and if so, of which categories of) special categories of personal data are used for profiling'

Concerning g) 'the processing applied'

The EDPB and the EDPS recall the broad definition of processing under the GDPR²⁸, and consider that

²⁸ Article 4(2) GDPR: “processing” means any operation or set of operations which is performed on personal data

gatekeepers may benefit from further clarifications as to the specific types of processing activities for which the Commission is seeking information on as they relate to consumer profiling techniques.

The EDPB and the EDPS recommend clarifying that the audited description regarding the ‘processing applied’ by the gatekeeper shall contain a complete description of the data lifecycle - from the moment of initial data collection until the moment of data erasure or destruction - and of the profiling techniques applied. This should cover, at least, all the stages of the consumer profiling process, specifically when gatekeepers collect data, analyse data, build a profile for an individual, and apply a profile to make a decision affecting the individual²⁹.

In addition, the EDPB and the EDPS recommend that the Commission explains in a footnote that gatekeepers should provide under this point an exhaustive description of the profiles applied to consumers, the description of the features or functionalities of the core platform service associated to those profiles, and whether the profiling is carried out directly by the gatekeeper or by another (named) entity (acting either on behalf of the gatekeeper as a processor, or as a separate/joint controller).

Concerning h) ‘whether automated decision-making takes place on the basis of an applied profiling technique, the number and object of such automated decisions, the legal effects³⁰ the automated decision making mechanism is producing or may produce, and a description of the algorithms underpinning the automated decision mechanism’

The EDPB and the EDPS recall that some instances of profiling can partially overlap with or result in automated decision-making affecting the rights and freedoms of data subjects to an extent that they would render them prohibited under Article 22(1) GDPR, in the absence of an applicable exception under Article 22(2) GDPR³¹. However, it is equally possible that the profiling does not, in itself, constitute or involve automated decision-making³².

or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

²⁹ [Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 \(WP251rev.01\)](#), as last Revised and Adopted on 6 February 2018, page 12.

³⁰ ‘A decision produces legal effects when the subject’s legal rights are impacted. This could include, for example, any resulting effect on their right to vote, their ability to take out a loan, and their position in recruitment.’

³¹ Opinion of Advocate General Pikamae of 16 March 2023, *OQ contre Land Hessen, en présence de SCHUFA Holding AG* (C-634/21), ECLI:EU:C:2023:220, which argues that the automated establishment of a probability value concerning the ability of the person concerned to service a loan in the future already constitutes a decision based solely on automated processing, including profiling, which produces legal effects concerning that person or similarly significantly affects him or her, where that value, determined by means of personal data relating to that person, is transmitted by the controller to a third-party controller and the latter, in accordance with consistent practice, draws strongly on that value for its decision on the establishment, implementation or termination of a contractual relationship with that same person.

³² [Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 \(WP251rev.01\)](#), as last Revised and Adopted on 6 February 2018, page 8: “Automated decision-making has a different scope and may partially overlap with or result from profiling. Solely automated decision-making is the ability to make decisions by technological means without human involvement. (...) Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used. (...) Decisions that are not solely automated might also include profiling. For example, before granting a mortgage, a bank may consider the credit score of the borrower, with additional meaningful intervention carried out by humans before any decision is applied to an individual.”

The EDPB and the EDPS would find it appropriate to enlarge the scope of point h) of Section 2.1. of the template, to include information related to both profiling and automated decision-making, as the concepts are different, yet both concepts are relevant to assess the potential negative effects of the gatekeeper's practices.

Additionally, the EDPS and the EDPB consider that the audited description of profiling techniques under Article 15 DMA should provide visibility over the effects that profiling techniques applied by the gatekeepers and automated decision-making based on such profiling may have on consumers, not only where gatekeepers understand that they qualify as "legal" effects.

If implemented, the footnote in point h) of Section 2.1. outlining examples of the types of effects that profiling or automated decision-making may have on consumers should therefore not focus solely on "legal" effects but also other types of significant effects. In any event, the EDPB and the EDPS note that the examples concerning the ability of individuals to take out a loan or success in e-recruitment processes currently included in the explanatory footnote could be seen not as 'legal' effects but 'similarly significant' effects³³. Therefore, the EDPB and the EDPS recommend amending the footnote accordingly.

Lastly, the EDPB and the EDPS recommend the inclusion of a footnote providing examples of the types of information that the Commission expects to receive with regards to the description of the algorithms underpinning the gatekeepers' profiling processes and automated decision-making schemes. Clear examples may help gatekeepers to identify the information sought and provide useful insights regarding their techniques, without necessarily revealing trade secrets. In this context, some examples could include the information such as why the gatekeeper considers the selected categories of data under points c) and d) of Section 2.1. of the template to be pertinent, how consumer profiles are built (including any statistics used), and why the profile is relevant for automated decision-making processes³⁴.

In light of the above, the EDPB and the EDPS recommend redrafting point h) of Section 2.1. of the template as follows:

*'whether automated decision-making takes place on the basis of an applied profiling technique, the number and object of such automated decisions, the legal, **similarly significant and other types** of effects the automated-decision making mechanism **and the profiling techniques are** producing or may produce, and a description of the algorithms underpinning the automated decision mechanism **and the profiling techniques'***

Concerning i) 'qualitative and quantitative impact or importance of the profiling techniques in question for the business operations of the gatekeeper'

Recital (72) DMA states that the audited description of gatekeepers' consumer profiling techniques should contain the "*impact of such profiling on the gatekeeper's services*". This does not necessarily

³³ Recital (71) GDPR. See also [Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 \(WP251rev.01\)](#), last Revised and Adopted on 6 February 2018, page 22: "It is difficult to be precise about what would be considered sufficiently significant to meet the threshold, although the following decisions could fall into this category: decisions that affect someone's financial circumstances, such as their eligibility to credit; decisions that affect someone's access to health services; decisions that deny someone an employment opportunity or put them at a serious disadvantage; decisions that affect someone's access to education, for example university admissions."

³⁴ [Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 \(WP251rev.01\)](#), As last Revised and Adopted on 6 February 2018, page 31.

correspond to the ‘business operations’ of the gatekeeper as currently mentioned in point i) of Section 2.1. of the template.

Therefore, the EDPB and the EDPS recommend redrafting point i) of Section 2.1. of the template as follows:

‘qualitative and quantitative impact or importance of the profiling techniques in question for the core platform services and other services of the gatekeeper, as well as the business operations of the gatekeeper’

In addition, the EDPB and EDPS recommend the Commission to further clarify which specific quantifiable information it seeks regarding the impact or importance of the profiling techniques for the business operations of the gatekeeper (e.g., the frequency with which profiles are applied, the number of advertising campaigns that relied on the use of profiling techniques, listing business areas or units which rely on the use of profiling techniques, or other types of correlation between the use of consumer profiling techniques and the business operations of the gatekeepers).

Concerning j) ‘actions taken to effectively enable consumers to be aware that they are undergoing profiling and the relevant use of such profiling’

The EDPB and the EDPS recommend asking gatekeepers to share the information that they provide to consumers about the profiling techniques they apply, as well as the format and the timing of such notice or description. To be clear, this information should not be restricted to automated decision-making, including profiling, within the meaning of Article 22(1) GDPR, but should also cover profiling that does not produce the types of effects covered by Article 22(1) GDPR³⁵.

The EDPB and the EDPS recall that the GDPR requires controllers to inform data subjects about various elements related to the processing of their personal data, including about the existence of specific types of automated decision-making and profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject³⁶.

Furthermore, the EDPB and the EDPS stress that it may be appropriate or necessary for gatekeepers to provide consumers with additional controls and corresponding information in relation to whether or how they carry out profiling, notably by giving consumers the possibility of adjusting or selecting the parameters that gatekeepers rely on for profiling³⁷. Details on the transparency that gatekeepers provide on the offered controls could inform supervisory authorities on the measure of data subjects’ control over the use of their personal data in core platform services.

The EDPB and the EDPS recommend redrafting point j) of Section 2.1. of the template as follows:

³⁵ Recital 60 GDPR refers to the obligation to disclose the purposes of processing (under Article 13(1)(c) GDPR), including when the purpose is profiling and even if the profiling is not covered by Article 22 GDPR. See [Article 29 Data Protection Working Party Article 29 Working Party Guidelines on transparency under Regulation 2016/679 \(WP260 rev.01\)](#), As last Revised and Adopted on 11 April 2018, paragraph 41.

³⁶ Articles 13(2)(f) and 14(2)(g) GDPR. For further detail, see [Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 \(WP251rev.01\)](#), last Revised and Adopted on 6 February 2018, pages 25, 26 and 31.

³⁷ For example, the EDPB and EDPS note that gatekeepers that qualify as providers of very large online platforms and of very large online search engines and that use recommender systems shall provide at least one option for each of their recommender systems that is not based on profiling, under Article 37 DSA. However, certain gatekeepers may provide more granular control to end users about how (and not only if) they are profiled, in line with key data protection principles such as fairness and data protection by design.

'actions taken, including copies of information provided, to effectively enable consumers to be aware that they are undergoing profiling, to be aware of the profiling techniques applied, and the relevant use, underlying logic and envisaged consequences of such profiling, the consumers' rights, as well as any options provided by gatekeepers in relation to such profiling'

Concerning k) where consumer consent is required for the given purpose under Regulation (EU) 2016/679, Directive 2002/58/EC and/or Regulation (EU) 2022/1925, a description of any steps taken to seek such consent to profiling, including details on how consumers can refuse consent or withdraw it, and any consequences of such refusal or withdrawal;³⁸

First, the EDPB and the EDPS recommend moving this point upwards in the list under Section 2.1. to logically follow point b) concerning the GDPR lawful grounds that gatekeepers rely on to carry out consumer profiling in their core platform services.

Secondly, the EDPB and the EDPS note that, in some situations - like when the processing involves special categories of data or constitutes automated decision-making covered by Article 22(1) GDPR - the threshold for valid consent is higher, as it must also be "explicit". Given the practical implications of this distinction regarding the level of formality required from controllers to obtain valid consent from data subjects³⁹, the EDPB and the EDPS recommend underlining this distinction in the template, so that the gatekeepers describe the extra efforts undertaken to ensure that consent is explicit when this is required.

Thirdly, the EDPB and the EDPS consider it appropriate for the Commission to seek from gatekeepers the specific wording, design and format gatekeepers use when requesting consent from data subjects in relation to their profiling techniques, including a visual representation thereof, and information about the moment when such consent is sought⁴⁰.

Therefore, the EDPB and the EDPS recommend redrafting point k) of Section 2.1. of the template as follows:

'where consumer consent or explicit consent is required for the given purpose under Regulation (EU) 2016/679, Directive 2002/58/EC and/or Regulation (EU) 2022/1925, a description of any steps taken to seek such consent to profiling, including a copy and visual representation of the consent requests presented to consumers, the moment in which consent is requested from consumers, details on how consumers can refuse consent or withdraw it, and any consequences of such refusal or withdrawal'

Concerning l) 'statistics on how many consumers choose to undergo profiling if they are given a choice'

To clarify the scope of the information sought by the Commission in relation to this point, the EDPB

³⁸ "It should be clear from the description what measures (e.g. in design) the gatekeeper takes to guarantee a neutral presentation of choices to the end user, and the level of facility or ease (e.g. how many clicks) for an end user to refuse or change their consent. The consequences of such refusal or withdrawal should also be clear from the description."

³⁹ [EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1](#), Adopted on 4 May 2020, Section 4.

⁴⁰ The EDPB and EDPS suggest, insofar as relevant, to offer gatekeepers the possibility of providing the materials requested under point j) and k) together (to the extent such visuals relate to how consent for processing is requested). In any event, gatekeepers should be requested to provide a complete overview of the user engagement flow.

and the EDPS recommend first asking gatekeepers whether they make available to consumers a version of their core platform service that does not involve profiling, and what are the conditions for consumers to access such version. Information on such conditions may serve as a relevant factor when assessing whether consent to carry out profiling was freely given and, thus, valid, notably where strong network effects are present in the gatekeeper's market⁴¹ or the gatekeeper enjoys a dominant position⁴².

The EDPB and the EDPS recommend redrafting point l) of Section 2.1. of the template as follows:

'statistics on how many consumers choose to undergo or not to undergo profiling, information on the version(s) of the core platform service which does not involve profiling, as well as a detailed description of the specific conditions that apply to consumers that opt for such version(s) (e.g. access to different or limited content, paid access) and information on which version is the default, if any, if they are given a choice'

Concerning m) 'whether and when the profiling technique has been the object of a data protection impact assessment⁴³ and the conclusion of such assessment'

The EDPB and the EDPS underline the important role of data protection impact assessments ('DPIAs') under Article 35 GDPR as an accountability tool for controllers in relation personal data processing activities that are likely to result in a high risk to the rights and freedoms of natural persons⁴⁴.

In many instances of profiling by gatekeepers, a DPIA would be required, either because the data processing would fall directly under Article 35(3)(a) of the GDPR, or because it would fulfil at least two of the criteria laid out in the EDPB guidelines on DPIAs (e.g., evaluation or scoring, processing of sensitive personal data, large scale processing, vulnerable data subjects given imbalances of power in digital markets)⁴⁵. The EDPB and the EDPS suggest that the explanatory footnote to point m) of Section 2.1. of the template include a reference to these EDPB guidelines.

Access by the Commission and supervisory authorities to the summaries of the DPIAs carried out by gatekeepers - and not merely to their conclusions - in relation to their profiling techniques could

⁴¹ [EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1](#), Adopted on 4 May 2020, paragraph 24: "Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by the WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will."

⁴² Judgment of the Court of Justice of 4 July 2023 *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)* (C-252/21), ECLI:EU:C:2023:537, paragraphs 149 and 150: "149. Furthermore, the existence of such a dominant position may create a clear imbalance, within the meaning of recital 43 of the GDPR, between the data subject and the controller, that imbalance favouring, inter alia, the imposition of conditions that are not strictly necessary for the performance of the contract (...) 150. Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations."

⁴³ "A data controller must carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 in certain circumstances that may also involve profiling."

⁴⁴ See Article 35(7) GDPR.

⁴⁵ [Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 \(WP 248 rev.01\)](#), As last Revised and Adopted on 4 October 2017, pages 9-11.

provide regulators with much needed transparency concerning how gatekeepers have considered and addressed the risks for data subjects that may arise from personal data processing in that context.

Therefore, the EDPB and the EDPS recommend redrafting point m) of Section 2.1. of the template as follows:

'whether, ~~and when~~ and why the profiling technique has or has not been the object of a data protection impact assessment, a summary ~~and the conclusion~~ of such assessment, information about how often the assessment is reviewed and updated, and the measures implemented by the gatekeeper to address the risks to the rights and freedoms of data subjects identified in such assessment'

Concerning n) and o) 'any alternative measures to profiling that have been implemented and their description, including reasons for choosing them,⁴⁶ alternative measures to profiling that have been considered and the reasons for not choosing them'

As also mentioned under point j), the EDPB and EDPS consider that it would be appropriate to seek information about why gatekeepers have or have not provided consumers with additional controls in relation to how they are profiled in core platform services, like enabling consumers to adjust or select the parameters that gatekeepers rely on for profiling purposes.

Therefore, the EDPB and the EDPS recommend redrafting points n) and o) of Section 2.1. of the template as follows:

'any alternative measures to profiling that have been implemented and their description, as well as additional controls for consumers in relation to how consumers are profiled, including reasons for choosing them; alternative measures to profiling, or additional controls for consumers in relation to how they are profiled, that have been considered and the reasons for not choosing them'

5. RECOMMENDATIONS FOR ADDITIONAL POINTS IN SECTION 2.1

As mentioned above, one of the goals of the Commission's transmission of the audited description of consumer profiling techniques to the EDPB is to inform the enforcement of Union data protection rules. In order to increase transparency and accountability in this context, the EDPB and the EDPS recommend enlarging the scope of the elements of information that the current wording of the template would require gatekeepers to provide to the Commission.

In particular, the EDPB and the EDPS highlight the importance of having gatekeepers clearly identify special categories of personal data⁴⁷ that are provided by consumers in a broad sense (i.e., both data which is actively provided by data subjects and data that is observed from their online activities) and that gatekeepers derive or infer based on the data that are provided by consumers or observed by gatekeepers, in the light of recent CJEU case law⁴⁸.

⁴⁶ "Asking for alternatives to profiling allows assessing whether gatekeepers have considered less intrusive measures and is particularly informative in terms of accountability."

⁴⁷ Article 9(1) GDPR.

⁴⁸ Judgment of the Court of Justice of 1 August 2022 *OT v Vyriausioji tarnybinės etikos komisija*, C-184/20, ECLI:EU:C:2022:601, paragraphs 118 and 127: "Article 9(1) of the GDPR provide for the prohibition, inter alia, of processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of data concerning a natural person's sex life or sexual orientation"; Article 9(1) GDPR "cannot be interpreted as meaning that the processing of personal data that are liable indirectly to reveal sensitive information concerning a natural person is excluded from the strengthened

In addition, the EDPB and the EDPS recommend including in Section 2.1. specific points on:

- *how the rights of data subjects under Chapter III of Regulation 2016/679 are ensured, a description of the technical and organisational measures in place that ensure that consumers can exercise these rights, especially when personal data has been combined from different sources;*
- *whether the gatekeeper transfers personal data to a third country or international organisation within the context of the processing applied for consumer profiling and, if applicable, the ground(s) under Chapter V GDPR that the gatekeeper relies on to carry out such transfers and a description and copy of the appropriate safeguards applied by the gatekeeper;*
- *a detailed description of the special categories of data processed by the gatekeeper in the context of consumer profiling (in particular, distinguishing special categories of data actively provided by consumers from observed special categories of data and from derived or inferred special categories of data); and*
- *the third parties involved in the processing and their role in that regard, as well as the recipients⁴⁹ of personal data, if any.*

6. COMMENTS TO SECTION 3.1. OF THE TEMPLATE

Concerning b) ‘overview of the professional qualifications, including domains of expertise, certifications, as applicable and descriptions of the responsibilities and work the respective member undertook during the audit’

The EDPB and the EDPS consider that an explanatory footnote in point b) of Section 3.1. of the template could point towards existing and available standards for auditors' professional qualifications⁵⁰, as a way of illustrating the level of expertise that the Commission expects auditors to have.

Concerning c) ‘declaration of interests by each auditing organisation, which contributed to the drafting of the submitted description, specifying in particular any relationship (including commercial or contractual) to the audited gatekeeper’

The EDPB and the EDPS also recommend the inclusion of an explanatory footnote in point c) of Section 3.1. of the template with a reference to applicable EU law on the prevention of conflicts of interests

protection regime". See also Judgment of the Court of Justice of 4 July 2023 *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social, C-252/21, ECLI:EU:C:2023:537*, paragraphs 68, 78 and 79: "For the purposes of applying Article 9(1) of the GDPR, it is important to determine, where personal data is processed by the operator of an online social network, if those data allow information falling within one of the categories referred to in that provision to be revealed"; "as regards, first, visits to websites or apps to which one or more of the categories referred to in Article 9(1) of the GDPR relate, it should be noted that the user concerned does not in any way thereby intend to make public the fact that he or she has visited those sites or apps and the data from those visits which can be linked to his or her person"; "Thus, it cannot be inferred from the mere visit to such websites or apps by a user that the personal data in question were manifestly made public by that user within the meaning of Article 9(2)(e) of the GDPR."

⁴⁹ Article 4(9) GDPR.

⁵⁰ As an example, see ISO/IEC 17065:2012(en) Conformity assessment — Requirements for bodies certifying products, processes and services, point 6.1.2.1.

in statutory audits⁵¹ as a point of reference on the independence of the auditors from the audited party (i.e., the gatekeeper).

7. COMMENTS TO SECTION 4.1. OF THE TEMPLATE

Concerning ‘A description of the audit procedures performed by the independent auditor or auditing organisation, the methodologies used to perform the audit (including, where applicable, a justification for the choice of standards, benchmarks, sample size(s) and sampling method(s))’

The below recommendations are without prejudice to the fact that the EDPB and the EDPS stress that the template should not serve as a replacement for the implementing act which the Commission may adopt pursuant to Articles 15(2) and 46(1)(g) DMA to develop the methodology and procedure of the audit.

The EDPB and the EDPS consider that point 4.1. could serve an opportunity for the Commission to illustrate the degree of independence it expects gatekeepers' auditors to have. This could be achieved via an example in an explanatory footnote to existing standards for assessing auditors' independence⁵².

The EDPB and the EDPS are also concerned about the current absence of specific Commission-vetted quality standards for gatekeeper audit methodologies. This entails the risk that the test and detail levels of each gatekeepers' audits pursuant to Article 15(1) DMA will vary considerably before the Commission adopts the implementing act under Articles 15(2) and 46(1)(g) DMA. Therefore, the EDPB and the EDPS recommend including an explanatory footnote in point 4.1. to provide examples of well-known audit methodologies that gatekeepers may leverage⁵³.

8. COMMENTS TO SECTION 5.1. OF THE TEMPLATE

Concerning a) ‘an assessment of “positive”, “positive with comments”, or “negative”, that the description provided is based on sufficient evidence derived from sufficient information provided by the gatekeeper’

The EDPB and the EDPS recommend replacing the reference to ‘sufficient information’ with ‘complete and accurate information’.

9. RECOMMENDATION FOR ADDITIONAL POINT IN SECTION 5

The EDPB and the EDPS recommend that gatekeepers be required to share with the Commission the final audit report(s) produced by the auditor(s) or auditing organisation(s). This disclosure under Article 15(1) DMA could be limited to the strict extent necessary to observe the rights and freedoms

⁵¹ Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts *OJ L 158, 27.5.2014, p. 196–226*, Article 1(14). See also Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC.

⁵² As an example, see ISO/IEC 17065:2012(en) Conformity assessment — Requirements for bodies certifying products, processes and services, point 4.2.

⁵³ As a possible example, see ISO/IEC 17020:2012(en) Conformity assessment — Requirements for the operation of various types of bodies performing inspection.

of third parties, including trade secrets. To this effect, the EDPB and the EDPS suggest that the Commission adds a new point 5.2. to Section 5.

Opinion of the Board (Art. 70.1.b)

Art.70.1.b

**Opinion 23/2018 on Commission proposals on European
Production and Preservation Orders for electronic evidence
in criminal matters (Art. 70.1.b)**

Adopted on 26 September 2018

Contents

Introduction.....	3
1. Legal basis of the Regulation proposal (article 82 TFUE)	4
2. Necessity of e-Evidence compared to MLATs and EIO.....	5
a) The necessity of e-Evidence compared to the safeguards provided by EIO and MLATs	5
b) The abandonment of the dual criminality principle.....	6
c) The consequence of addressing the companies directly	7
3. The new ground for jurisdiction and the so-called disappearance of the location criteria	8
4. The notion “service providers” should be restricted or complemented by additional safeguards for the data subjects’ rights	9
5. The notions of “establishment” and of “legal representative” in the context of these proposals should be clearly distinguished from these notions in the context of the GDPR	10
a) Establishment.....	10
b) Legal representative.....	11
6. New categories of data.....	11
7. Analysis of the procedures for European Preservation and Protection Orders.....	13
a) Thresholds for issuing orders should be raised and orders shall be issued or authorised by courts.....	14
b) Time-limits to provide data should be justified	15
c) European Production and Preservation orders shall not be used to request data of another Member State data subject without at least informing the competent authorities of that Member State, in particular for content data.....	16
d) European preservation orders shall not be used to circumvent data retention obligations of the service providers	16
e) Confidentiality and user information	16
f) Procedure for the enforcement of an order when the service provider refuses to execute it	17
g) Enforcement of orders and conflicting obligations under third country laws (articles 15 – 16)	
17	
h) Security of data transfers when responding to an order	19
Conclusions.....	20

The European Data Protection Board

Having regard to Article 70 (1b) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

HAS ADOPTED FOLLOWING OPINION:

Introduction

In April 2018, the Commission presented a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and a proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purposes of gathering evidence in criminal proceedings. The two proposals COM(2018) 225 final and COM(2018) 226 final are complementary. The overall goal pursued by the Commission is to improve cooperation between Member State authorities and services providers, including those based in non-EU countries, and to propose solutions to the problem of determining and enforcing jurisdiction in cyberspace.

While the draft Regulation foresees the rules and procedures applicable to issue, serve and enforce preservation and production orders on providers of electronic communication services, the draft Directive provides for minimum rules for the appointment of a legal representative for service providers not established in the EU.

In November 2017¹, before the Commission tabled any draft proposal, the Article 29 Working Party (WP29) recalled the necessity to ensure that any legislative proposal fully complies with the existing EU data protection *acquis* in particular, as well as EU law and case-law in general.

In particular, the WP29 warned against limitations to the rights to data protection and privacy with respect to data processed by telecommunications and information society providers, especially when further processed by law enforcement authorities, recalled the necessity to ensure consistency of any EU instrument with the existing Council of Europe Budapest Convention on cybercrime and with the EU Directive on the European Investigation Order (EIO), and recommended to clarify the respective procedural rules governing access to e-Evidence at national and EU level to ensure that the new instrument would not grant authorities new powers they would not have internally. In addition to these general remarks, the WP29 commented on the legislative options considered by the Commission at that time concerning the categories of data concerned and the corresponding safeguards to access them, on the possibility to address production orders/requests to compel service providers to provide data located outside the EU, and on the substantive and procedural conditions necessary safeguards to surround direct access to data.

With the concrete proposals on e-Evidence at hand now, the EDPB wishes to give a more detailed analysis of the proposed legal instruments from a data protection point of view.

¹ See WP 29 statement (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

1. Legal basis of the Regulation proposal (article 82 TFUE)

The legal basis suggested for the e-Evidence draft Regulation is article 82(1) of the TFEU, concerning judicial cooperation in criminal matters, which provides:

“1. Judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 83.

The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures to:

- (a) lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions;*
- (b) prevent and settle conflicts of jurisdiction between Member States;*
- (c) support the training of the judiciary and judicial staff;*
- (d) facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions.”*

As underlined by the Commission in the impact assessment accompanying the proposals, “Article 82(1) specifies that judicial cooperation in criminal matters shall be based on the principle of mutual recognition. This legal basis would cover possible legislation on direct cooperation with service providers, in which the authority in the issuing Member State would directly address an entity (the service provider) in the executing State and even impose obligations on it. This would introduce a new dimension in mutual recognition, beyond the traditional judicial cooperation in the Union, so far based on procedures involving two judicial authorities, one in the issuing State and another in the executing State.”(emphasis added)

Given the novelty of the use of this legal basis in the context of direct requests between public authorities and private parties, the EDPB regrets that no further analysis nor assessment is provided by the Commission.

Indeed, as already underlined by the Working Party in its previous statement, the EDPB continues to stress its doubts on the appropriateness of this legal basis, which are supported by the analysis of the CJEU and its Advocate General in the Opinion 1/15. Among the developments made concerning the validity of Article 82 as a legal basis for the draft PNR agreement between the EU and Canada, the Court underlined that the Canadian Competent authority “*does not constitute a judicial authority, nor does it constitute an equivalent authority*”². In the context of the e-Evidence proposals, one of the main goal pursued as stated by the Commission appears to be to avoid the “too cumbersome” judicial cooperation. Consequently, the proposal is based on the principle that cooperation should take place between an authority and a service provider rather than between two authorities. The procedure foreseen primarily places private entities in the position to be the receiving party and to answer the requests emanating from judicial authorities.

The EDPB notes that the process of enforcing production or preservation orders could imply the involvement of a receiving authority in the situation where the receiving service provider does not comply with its obligations and will thus trigger the need to call for an ex-post enforcement of the order. However, as the main objective of the procedure set up is precisely not to involve a receiving

² See point 103 of Opinion 1/15 and point 108 of the opinion of the advocate general in this case.

authority, the EDPB doubts that this ancillary procedure could justify the use of Article 82 as the sole legal basis for the instrument.

Therefore, the EDPB takes the view that for Article 82 to be used as a legal basis the main procedural steps of the cooperation shall take place between two judicial authorities and that another legal basis should be used for this type of cooperation.

2. Necessity of e-Evidence compared to MLATs and EIO

The EDPB notes that the Commission is committed to review obstacles to criminal investigation, especially regarding the issue of access to electronic evidence. In its explanatory memorandum, the Commission gives the context of the proposal and stresses the volatile nature of electronic evidence, its international dimension as well as the need to adapt cooperation mechanism to the digital age. Proposals for a regulation and a directive for transferring and accessing electronic evidence are not aiming to replace previous cooperation instruments in criminal matters such as the Budapest Convention, the Mutual Legal Assistance Treaty (MLAT) and the European Investigative Order (EIO directive). According to the Commission, e-Evidence proposals aim at improving judicial cooperation in criminal matters between authorities and service providers within the European Union as well as with third countries, the United States of America in particular.

Since these new additional tools will be specifically dedicated to the access and transfer of electronic evidence, the EDPB will assess the added value of the instruments regarding the EIO directive and the MLAT.

a) The necessity of e-Evidence compared to the safeguards provided by EIO and MLATs

The main argument raised by the Commission in favor of the e-Evidence proposals is to speed up the process to secure and obtain electronic evidence that is stored and/or held by service providers established in another jurisdiction.

The EDPB however deplores that the necessity to have a new instrument to organize access to electronic evidence was not demonstrated in the impact assessment. Indeed, the proposals lack a demonstration that no other less intrusive means could have been used to achieve the goal of the e-Evidence proposal, while alternative solutions could have been contemplated. For instance, the possibility to modify and improve the EIO Directive could have been examined and would also have answered the specific requirement under the EIO Directive to evaluate the need to amend the text by 21 May 2019³. Another option could have been to foresee the use of preservation orders to freeze the data for as long as a formal request based on an MLAT were issued. These options would have allowed to maintain the safeguards provided in these instruments while ensuring that the personal data sought is not deleted.

The EDPB notes that the time limits established in the EIO Directive are longer than in the e-Evidence proposal. Indeed, the executing authority has 30 days to take its decision on the recognition of the request⁴ and then should execute the order within 90 days⁵. The EDPB considers that allowing 30 days

³ See Art. 37 of the EIO Directive

⁴ Art. 12 (3) EIO Directive

⁵ Art 12 (4) EIO Directive

of reflection for the executing authorities in the EIO is a crucial safeguard enabling them to assess whether the request for execution is well founded and respects all the conditions for issuing and transmitting an EIO⁶.

The EDPB is concerned that the 10-day deadline put forward in the e-Evidence proposals to execute the European Production Order Certificate (EPOC), without any time for reflection, prevents the proper assessment of whether the EPOC meets all the criteria and is completed correctly.

Therefore, the EDPB recommends that more time be provided for the EPOC recipient to determine whether the order should or should not be executed.

The EDPB notes that in case of a European Preservation Order (EPOC-PR), there is no guaranty that the preservation of the data will be limited to what is necessary to produce. Indeed, the duration of preservation of the data may exceed 60 days since there is no time limit for the issuing authority to inform the addressee to refrain from issuing, or to withdraw a production order. Therefore, the EDPB recommends at least a time limit for the issuing authority to refrain or withdraw the production order in order to comply with the principle of data minimization established in the GDPR⁷.

Finally, the EDPB notes that the EIO directive establishes the return of evidence from the issuing State to the executing authority⁸. However, the E-evidence Regulation proposal is silent regarding such a possibility. What happens to the electronic evidence after its transmission to the issuing authority is unclear.

Therefore, the EDPB recommends that the Regulation proposal should provide more information on the use of electronic evidence after their transfer to the issuing authority in order to comply with the GDPR and the principle of transparency⁹ as well as the principle of specificity established by the MLATs.

b) The abandonment of the dual criminality principle

The EDPB acknowledges that mutual recognition is dependent on the application of the double criminality which is a way for Member States to maintain their sovereignty. However, double criminality is increasingly considered as an obstacle to smooth judicial cooperation. EU Member States are more and more willing to cooperate even if the investigative measures relate to acts that are not considered as an offence in their national law. The EDPB however recalls that the dual criminality principle aims at providing an additional safeguard to ensure that a State cannot rely on the assistance of another to apply a criminal sanction which does not exist in the law of another State. This would for instance prevent a State from requiring the help of another one to imprison someone for their political opinions if these opinions are not criminalized in the requested State or to prosecute someone for having aborted if this person is residing in another State where it is not illegal. The dual criminality principle is also often accompanied by additional limitations or safeguards concerning the sanctions if they differ too much between the requesting and the executing State. The main example is the commitment not to apply the death penalty in certain MLATs when it does not exist in the law of one of the two parties.

⁶ Art. 6 EIO Directive

⁷ Art. 5 (1) (c) GDPR.

⁸ Art. 13 (3) and (4) EIO Directive.

⁹ Art. 5(1) (a) GDPR.

The EDPB notes that the dual criminality principle is ruled out in the e-Evidence regulation proposal. However, it does not result only in the deletion of the usual formalities of mutual recognition but also in the deletion of safeguards linked to the dual criminality principle itself.

Indeed, the EDPB notes that no reference is made to the law of the country where the requested service provider is established, and that the preservation of any data, as well as the production of subscriber or access data, may be issued for all criminal offences¹⁰ regardless of whether there are similar criminal offences established in other Member States or not.

Meanwhile, production orders may only be issued and executed if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State¹¹. In addition, as explained by the Commission in the explanatory memorandum of the regulation proposal, the specificity of transactional data and content data is established, as they are considered to be more sensitive. Indeed, orders concerning transactional or content data are based on a threshold of a maximum custodial sentence of at least 3 years in order to ensure respect for proportionality and the rights of the persons affected¹². However, the EDPB underlines that no harmonization within the EU has taken place yet of criminal offences punished by a maximum of at least 3 years of custodial sentence.

The EDPB opposes the abandonment of the dual criminality principle, which aims at ensuring that a State cannot rely on the help of others to have its national criminal law applied outside of the State's territory by a State which does not share the same approach, especially given the disappearance of other traditional major safeguards in the field of criminal law (see below point 3 on the location criteria and point 7 (g) concerning potential conflicts with third countries' laws).

c) The consequence of addressing the companies directly

The EDPB acknowledges that electronic evidence is increasingly available on private infrastructure and may be located outside the investigating country, owned by service providers.

The EDPB notes that following the *Yahoo!*¹³ and *Skype*¹⁴ decisions in Belgium and in the context of terrorist attacks, there is a need for a smoother and faster cooperation between public and private entities. In the impact assessment, the Commission refers to three types of procedural instruments involving both public authorities and service providers. These are judicial cooperation, direct cooperation and direct access. If the first one is not putting the responsibility on the service provider to execute the EIO but on the executing authority¹⁵, the second, direct cooperation, is based on the cooperation of the service provider. The most intrusive is direct access from a service provider's perspective since public authorities are able to access data without the help of an intermediary.

Therefore, the EDPB fears that, when addressed directly, service providers will not ensure the protection of personal data as efficiently as public authorities are able and obliged to do and stresses that it also results in the inapplicability of certain procedural guarantees foreseen in the context of

¹⁰ Art. 5 (3) and Art. 6 (2) of the proposed Regulation on e-Evidence.

¹¹ Art. 5 (2) of the proposed Regulation on e-Evidence

¹² Art. 5 (4) (a) of the proposed Regulation on e-Evidence

¹³ Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1st December 2015.

¹⁴ Correctieonele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016. (Skype has appealed the decision).

¹⁵ Art. 10 – 16.

judicial cooperation for individuals, as well as for companies themselves¹⁶. Indeed, for instance, a requested service provider would have to go before the court of another (Member) State to contest the order while in the context of judicial cooperation it would face its own authorities. The EDPB recommends the inclusion of additional grounds in the Regulation proposal certifying that service providers will protect individual fundamental rights as the protection of personal data and the respect of private and family life, as well as the information of the competent data protection authority in order to make sure control is possible.

3. The new ground for jurisdiction and the so-called disappearance of the location criteria

The EDPB notes that the Commission underlines that one of the major changes brought by these proposals is the disappearance of the location criteria and the possibility for competent authorities to request the preservation and production of data regardless of where these data are actually stored.

From a data protection perspective, it is not new that EU data protection law applies regardless of where the data of persons concerned are stored. Indeed, the applicability of the GDPR depends either on the fact that the controller or processor is established within the EU, or on whether EU data subjects' data are processed, even when the controller or processor are not established on the territory of the EU¹⁷, in which case they also have to designate a legal representative in the EU¹⁸. From the perspective of data protection it is important to note that the extended territorial scope aims at providing a more complete protection to EU data subjects, regardless of where the company processing their data is established.

Therefore, although the disappearance of the location criteria might be new in the field of criminal law, this does not appear as a major change from a data protection perspective. In addition, the EDPB also notes that a link is still maintained with the territory of the EU as only service providers offering services in the Union fall within the scope of the proposals, and the fact that requests can only be addressed in the context of criminal investigations imply a link with the EU (either because the crime was committed in the territory of a Member State or because the victim or the criminal was a citizen of a Member State).

If the disappearance of the location criteria should now be applied in criminal law, the most important question for the EDPB concerns how to ensure that such a development is not detrimental to data protection and criminal procedural rights of the data subjects and the requested service providers. From that perspective, the EDPB acknowledges that within the EU, procedural safeguards have been, at least partially, harmonized and need to be provided in compliance with the European Convention of Human Rights. It can thus be argued that the disappearance of the location criteria would probably have more limited consequences when the evidence is sought within the EU compared to the reverse situation where authorities from third countries request data to companies established within the EU under the same conditions as set out in the e-Evidence draft Regulation. Indeed, the EDPB is particularly concerned this could result in more problematic situations. In this context, authorities from

¹⁶ See also from an international data protection perspective the "Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes", The International Working Group on Data Protection in Telecommunications, 63rd meeting, 9-10 April 2018, Budapest (Hungary).

¹⁷ See Art. 3, in particular (2).

¹⁸ See Art. 27

a third country where different and potentially less procedural safeguards apply in the field of criminal law could have access to data that would be protected by additional safeguards within the EU. From that perspective, the EDPB recalls its concerns about a double standard and a weakening of fundamental rights when service providers and data subjects do not benefit from the procedural safeguards in EU law if the request is made from a third country authority.

Furthermore, as this new ground of jurisdiction “regardless of the location of the data” is coupled with a procedure mainly relying on direct requests from competent authorities to service providers, the EDPB is concerned that data protection safeguards may not be applied by private companies receiving requests and which are not bound by a legal instrument such as an MLAT, traditionally governing the exchanges of data between judicial authorities and providing for safeguards. In particular, in the context of MLATs, minimum data protection safeguards imply for instance confidentiality obligations and the principle of specificity which implies that data will not be processed for another purpose.

At least, the EDPB therefore recalls that the safeguards provided in Directive 2016/680 should be made applicable, including with regards to data transfers, and especially Article 39 in case the service provider would be established in a third country without an adequacy decision in this field. In particular, the EDPB stresses that this provision implies notably the information of the competent data protection authority in the Member State of the issuing authority of the order(s) and the documentation of the transfer, including with regards to the justification concerning the ineffectiveness or inappropriateness of a transfer to the competent authority of the third country.

4. The notion “service providers” should be restricted or complemented by additional safeguards for the data subjects’ rights

As regards service providers, the EDPB welcomes the wide definition which allows to include both communication services and Over-The-Top (OTT) services, since all these services are functionally equivalent and therefore the foreseen measures could have a similar impact on the right to privacy and the right to secrecy of communications, as underlined in the statement of the WP29 and previously in Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation. Indeed, the proposal for a Regulation on electronic evidence covers service providers providing either electronic communications services as defined in Article 2(4) of Directive establishing the European Electronic Communications Code, information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535, “for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users, and other hosting service providers”, or internet domain name and IP numbering services “such as IP providers domain name registries, domain name registrars and related privacy and proxy services”¹⁹.

However, a service provider in the sense of the draft Regulation being “any natural or legal person that provides one or more of the following categories of services”, the EDPB is concerned that this instrument could cover both controllers and processors in the sense of the GDPR. Indeed, as “offering services” as defined in Article 2 (4) of the draft Regulation includes both enabling legal or natural persons in one or more Member State(s) to use the services listed, and having a substantial connection

¹⁹ Article 2 (3) (c) of the proposed Regulation on e-Evidence

to the Member State(s) in question, these activities include activities performed by a processor for a controller, such as storing data, for instance.

Hence, the EDPB fears that without limitations to service providers acting as controllers in the sense of the GDPR, and without any specific obligation of the processor to notify the data controller, when addressed with a production or preservation order, data subjects' rights might be circumvented. This is especially the case since in the context of possible conflicting obligations preventing the addressee to serve the orders received, the judicial authorities are also encouraged in the draft Regulation itself to address the most appropriate actor regardless of the data protection rules applicable, in particular given that any data could be requested, and not only personal data subject to the GDPR²⁰.

According to the GDPR, a processor only acts on the instructions given by the controller. Therefore, it is the responsibility of the controller to ensure the rights of data subjects are respected, and to provide them with the relevant information, including with regards to recipients of their data, for instance in the context of the exercise of their right of access. The processor will not receive these requests from data subjects and will not be in a position to answer, unless expressly asked by the controller.

Consequently, unless their rights have been limited in application of the GDPR, the EDPB stresses that data subjects benefitting from the application of the GDPR may not be able to exercise their rights efficiently if the controller is not in a position to provide complete information. The EDPB also notes that the likelihood of the absence of information is even higher without any specific obligation imposed on the processor to inform the controller when the data requested concern data subjects who do not benefit from the protection granted by the GDPR. Indeed, the judicial authorities requesting the data will not necessarily have the obligation to inform the data subjects of their own further processing in this case. The EDPB therefore calls on the restriction of the scope to controllers in the sense of the GDPR, or on the introduction of a provision clarifying that in the event where the service provider addressed is not the controller of the data, it shall inform the controller.

5. The notions of “establishment” and of “legal representative” in the context of these proposals should be clearly distinguished from these notions in the context of the GDPR

Given the inapplicability of the location criteria with regards to data, the addressees of production and preservation orders within the scope of the proposed Regulation are limited to service providers offering services in the Union, whether established within the EU or not, with the obligation to appoint a legal representative, according to the rules proposed in the draft Directive. These notions of “establishment” and “legal representative” are therefore defined in the draft instruments.

The EDPB notes that these notions also appear in the context of other EU instruments, and in particular in the context of the GDPR. Consequently, clarifications as to the definition and delineation between these notions in the context of the draft proposals and in the context of the GDPR should be provided.

a) Establishment

The EDPB also recalls that the notion of “establishment” in the context of the draft Regulation shall not be confused with the notion in the context of the GDPR. Indeed, for the purpose of the draft

²⁰ See Article 7 (3) and (4)

Regulation, the notion of establishment as defined in Article 2 (5) is broader than in the GDPR as it includes “either the actual pursuit of an economic activity for an indefinite period through any stable infrastructure from where the business of providing services is carried or a stable infrastructure from where the business is managed”, whether or not processing of personal data takes place in the context of the activities of this establishment. Thus, if “establishment” in the sense of the GDPR was to undoubtedly be included in the establishment defined in the draft Regulation, the contrary might not be the case.

The EDPB therefore warns that establishments of service providers in the sense of the draft Regulation might not necessarily imply that the conditions for the application of the GDPR according to Article 3(1) are met. In this context, controllers and processors are therefore invited to check if the applicability of the GDPR does not derive from Article 3(2) which would imply the designation of a legal representative within the EU and the absence of One-Stop-Shop mechanism.

b) Legal representative

In its statement, the WP29 stressed that any confusion should be avoided between the obligation to designate a legal representative under Article 27 of the GDPR and the legal representative foreseen under the draft Regulation on e-Evidence.

With the draft proposal at hand, the EDPB would like to recall these recommendations, and in particular to underline that in its understanding, the legal representative in the meaning of the draft Directive on the appointment of a legal representative in the context of the e-Evidence proposals shall be designated in any case, be vested with specific functions, independently of a mandate given by the service provider, have the power to answer requests and to act on behalf of the service provider and a stronger liability than the legal representative of the GDPR.

Furthermore, the EDPB stresses that the obligation to designate a legal representative in any case under the e-Evidence draft proposals, whether the service provider is established in the EU or not, the possibility to designate even several legal representatives for the same service provider under the e-Evidence draft Directive, and the obligation to notify the designation of the legal representative to the Member States’ authorities differ from the GDPR, which does not provide for such obligation to notify the designated legal representative, exemptions to the designation and limited responsibilities of the legal representative.

Therefore, given the important differences in terms of role, liability and relationship with the other establishments of the service provider in one case and controller or processor in the other, the EDPB recommends that, where a service provider is not established within the EU, but is subject to both the GDPR pursuant to article 3 (2) and to the e-Evidence Regulation, two distinct legal representatives should be designated, each with clear distinct functions according to the instrument on the basis of which it is designated.

6. New categories of data

The proposed regulation defines different categories of data as per article 2: subscriber data, access data, transactional data and content data. Recital 20 of the Commission proposal further specifies that *“The categories of data this Regulation covers include subscriber data, access data, transactional data (these three categories being referred to as ‘non-content data’) and content data. This distinction, apart from the access data, exists in the legal laws of many Member States and also in the current US legal*

framework that allows service providers to share non-content data with foreign law enforcement authorities on a voluntary basis.”

In this context, the EDPB stresses first of all that all four categories of data cited above are to be considered as personal data according to EU data protection law since they do contain information related to an identified or identifiable natural person, whether the data subject is referred to as “subscriber” or “user” in the proposed regulation. Similarly, it is to be noted that “electronic evidence” as defined in Article 2(6) of the Commission’s proposal encompasses all four categories of data and therefore relates to personal data. Therefore rather than laying down the rules for access to evidence, defined and qualified as per national law and judicial procedures, the proposed regulation provides for new substantive and procedural conditions related to the access to personal data.

While the proposed regulation establishes new subcategories of personal data for which different procedural conditions of access apply, the EDPB recalls that, in accordance with the relevant CJEU case law, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way.

Furthermore, the EDPB recalls that in relation to “non-content data” which encompass subscriber data, access data and transactional data as per the Commission proposal, the Court of Justice of the European Union has ruled in its judgement in joined cases C-203/15 and C-698/15 *Tele2 Sverige AB* that metadata such as traffic data and location data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications²¹.

As already stated in the WP29 statement on Data protection and privacy aspects of cross-border access to electronic evidence of 29th November 2017, the EDPB therefore reiterates its doubts and concerns with regards to the current delineation between “non-content” and content data, as well as to the four categories of personal data laid down by the proposed regulation. Indeed, the four categories proposed do not appear to be clearly delineated, and the definition of “access data” still remains vague, compared to the other categories. The EDPB therefore regrets that the Commission’s impact assessment and proposal did not further substantiate the rationale for the creation of these new subcategories of personal data, and expresses its concerns with regards to the different level of guarantees related to the substantive and procedural conditions for access to the categories of personal data, especially given the practical difficulty to evaluate to which category of data will belong the requested data in some cases. For instance IP addresses could both be classed as transactional data and subscriber data.

In this context, the EDPB also recalls that in recital 14 of its proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy), the Commission considers that “electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication”. Since the current and future ePrivacy framework, as well as the related limitations to the right to privacy, will apply to the rules regulating law enforcement access

²¹ CJEU Judgment of 21 December 2016, paragraph 99.

to electronic evidence, the EDPB recommends that a broader definition of electronic communication data is included in the proposed regulation, in order to ensure that the appropriate safeguards and conditions for access to be established cover consistently both ‘non-content’ and ‘content data’.

7. Analysis of the procedures for European Preservation and Protection Orders

Broadly speaking, the procedure for addressing a production or preservation order appears to be the following:

- The competent judicial authority – the issuing authority – depending on the type of data requested and on the type of order, issues the order according to the (scarce) conditions enumerated in articles 5 and 6, sends it by using a harmonized certificate to the legal representative of the service provider or to any of its establishment within the EU – the addressee.
- Upon receipt of the certificate, the addressee shall execute the order – meaning transmit the data within 10 days or 6 hours in case of emergency, or preserve them up to 60 days – unless it is impossible do so, because the certificate is incomplete or because of *force majeure* or de facto impossibility for the addressee, or because the addressee refuses on the ground of conflicting obligations, either with regard to fundamental rights or fundamental interests of a third country or based on other grounds.
- In case the addressee has not complied with the order received without providing reasons accepted by the issuing authority, procedures are foreseen to enforce the orders by a competent enforcing authority in the Member State where the service provider is represented or established, unless limited grounds for refusal apply and the enforcing authority objects to the recognition or enforcement of the order.
- In case the addressee issued a reasoned objection to the order based on conflicting obligations, the issuing authority shall refer the case to the competent court in its Member State, which shall then be in charge of assessing the possible conflict and of upholding the order in the absence of a conflict. In the event of a conflict, the competent Court shall, either address the central authorities in the third country, via its national central authorities, with a 15 day deadline to respond, which can be extended by 30 days upon reasoned request, in case of conflicting obligations with regards to fundamental rights or fundamental interests of a third country, or determine itself whether to uphold or withdraw the order for other grounds of refusal invoked by the addressee.
- Without prejudice to remedies available under the GDPR and the LED, persons whose data was obtained via a production order shall also have the right to effective remedies against this order.

The EDPB assessed the procedures foreseen and the safeguards provided in the draft Regulation to surround the different steps and on each of the aspects presented here-after recommends the following safeguards and amendments.

a) Thresholds for issuing orders should be raised and orders shall be issued or authorised by courts

As regards the conditions for issuing orders, the EDPB welcomes the principle of higher safeguards to access transactional or content data. However, it notes that given the absence of full harmonisation of criminal sanctions between Member States, the reference to “criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years”²² still implies diverging thresholds and discrepancies in the protection of their data for data subjects within the EU.

Furthermore, the EDPB stresses that, especially given the broad definition of subscriber data, the threshold provided appears rather low for preservation orders and for production orders concerning subscriber or access data, as all criminal offences can in principle justify the issuance of such orders. Similarly, the authorities allowed to issue such orders are more limited in the context of production orders concerning transactional or content data, than for the issuance of preservation orders or production orders to produce subscriber or access data, as prosecutors can issue or authorise only the latter orders, while any judge, court or investigating judge can issue or authorise any order.

In particular, the EDPB regrets that the lowest threshold providing for the possibility for law enforcement authorities to request access to subscriber and access data for any criminal offence builds on an “*a contrario*” reading of the case law of the CJEU (which focuses on the other data) to make distinctions as the safeguards to be afforded. Indeed, the CJEU specifically underlined that for traffic and location data, access of the competent authorities shall be restricted solely to fighting serious crime²³. The EDPB could understand that the proposal would provide for the possibility to request access to very basic information which would just allow to identify a person without revealing any communication data without a prior authorisation from a court. However, it deplores the broad “*a contrario*” reading of this ruling by the Commission and calls for higher safeguards to be introduced in order to restrict the grounds for access to other subscriber data and to access data. The EDPB suggests to restrict access to these data either to a list of crimes provided in the draft Regulation, or at least to “serious criminal offences”, especially given the lower prior authorisation threshold foreseen for these data.

In addition, the EDPB underlines that this “*a contrario*” reading also leads to the fact that the proposal opens the possibility for prosecutors to issue or authorise the issuance of orders. The EDPB is of the opinion that, except in case of requests concerning very basic information which would just allow to identify a person without revealing any communication data, this constitutes a step back compared to the case law of the CJEU concerning access to communications data. Indeed, in its case law concerning access to communications data for law enforcement purposes, the CJEU has restricted the possibility to provide for such access, among other criteria, and “*except in cases of validly established urgency*”²⁴, to a “*prior review carried out by a court or an independent administrative authority*”, “*following a reasoned request of competent national authorities submitted within the framework of procedures of prevention, detection or criminal prosecution.*”²⁵

The EDPB recalls that the notion of “court” is an autonomous notion of EU law, and that the CJEU has constantly underlined and recalled the criteria to be fulfilled to qualify as a court, including the criteria

²² See Art. 5 (3) (a)

²³ See case 203/15 – Par (125)

²⁴ See case 203/15 – par (120)

²⁵ See joint cases C 293/12 and C 594/12 - par (62)

of independence²⁶ which does not appear to be the case for prosecutors, as recalled also by the ECtHR in its case law²⁷.

Consequently, articles 4 (1) (a) and (b) and 3(a) and (b) result in procedures where significantly less safeguards will apply for subscriber and access data since a prosecutor alone will be able to request data, without neither any further control from the authority of the State where the requested data are or from the authority where the legal representative of the requested company will be, nor any control from an independent administrative authority.

Furthermore, the EDPB notes the so-called additional safeguard provided in Article 5 (2) which limits the possibility to issue a production order when a similar measure was available for the same criminal offence in a comparable domestic situation. However, it warns against the counterproductive effect of such a provision: rather than providing additional safeguards it appears as an encouragement for Member States to extend their national possibilities to ask for the production of subscriber or access data in order to ensure production orders could be issued under this Regulation.

b) Time-limits to provide data should be justified

The EDPB notes that European Production orders shall be answered within 10 days at the latest upon receipt of the certificate, unless the issuing authority indicates reasons for earlier disclosure, and at the latest within 6 hours in emergency cases, as provided in Article 9 (1) and (2).

However, the EDPB has not seen any criteria framing the obligation for authorities to demonstrate the emergency to produce data, even *ex post* in order to allow for a possible control of the use of this very fast procedure, while a six hour deadline is likely to imply a very light control before producing the data, if not the absence of any control on the part of the service provider. Indeed, the impact assessment stresses the necessity for competent authorities to have access to data in a timely manner. However, the examples given in the impact assessment all concern evidence needed in case of serious crimes being committed (terrorism cases with hostages, ongoing child sexual abuse situations), but the justification based on the volatility of evidence does not appear to be a good one when there is no specific urgency other than this potential volatility of the data. In addition, the volatility of data does not provide any additional justification as to the proportionality to have access to data with less safeguards in these situations where there is no urgency other than the volatility of data.

In addition, the EDPB doubts the necessity to provide for a six hours deadline while providing that this deadline would not apply until the issuing authority provides additional clarifications "within five days" in case the service provider cannot comply with its obligation.

The EDPB therefore calls for additional elements in the impact assessment to justify the necessity of these deadlines in cases where the crime being committed or prosecuted is not serious, and unless such detailed elements are provided, for explicit criteria to justify the emergency in case EPOCs are issued. For instance, the same model as in the EIO Directive could be foreseen. The EIO Directive provides for a shorter deadline when justified by "procedural deadlines, the seriousness of the offence or other particularly urgent circumstances" (see Art. 12 (2)), or for a 24-hour deadline to decide on provisional measures (see Art. 32 (2)). Indeed the impact assessment of the draft Regulation does not provide for detailed elements to justify why these deadlines are not efficient, the only elements underlined being that the number of requests sent overload the receiving judicial authorities which cannot respect the deadlines.

²⁶ See for instance case C 203/14

²⁷ See for instance Moulin c/ France 23/11/2010

c) European Production and Preservation orders shall not be used to request data of another Member State data subject without at least informing the competent authorities of that Member State, in particular for content data

The EDPB recalls that in existing instruments judicial cooperation and thus additional safeguards, are provided, in particular to control the necessity and proportionality of requests, and underlines that these safeguards are all the more justified in cases where requested data are content data which involve more limitations of the rights of data subjects to have their personal data and privacy protected. In this regard, the EDPB recalls that the EIO Directive also provides for the possibility to intercept telecommunication with the technical assistance of another Member State (see Art. 30), as well as for the obligation to notify any interception of data to the competent authority of another Member State where no assistance is needed when the data subject concerned is or will be on the territory of that Member State (see Art. 31).

The EDPB finds no justification for the procedure foreseen in the draft e-Evidence Regulation to allow for the production of content data without any involvement at least of the competent authorities of the Member State where the data subject is.

d) European preservation orders shall not be used to circumvent data retention obligations of the service providers

The EDPB notes that the main aim of European Preservation Orders is to prevent data from being erased.

Although the EDPB recognizes that it may be necessary and proportionate in some cases, it deplores the lack of safeguards surrounding the issuance of such orders. In particular, the EDPB recommends that when preservation orders are addressed for specific data only, where the draft seems to allow for broad requests, and that when such orders are issued for data scheduled to be erased in compliance with the data retention principle, the order shall never serve as a basis for the service provider to process the data after the initial date of erasure. In other words, data should be “frozen”.

In addition, the link between the preservation order and the subsequent request for the production of data, be it through a European Production order, an EIO request or a mutual legal assistance request, should be strengthened, in order to ensure that European Preservation orders are issued only when the other request is certain (and not just contemplated as a possibility), and that when the other request is refused, the preservation order also expires, without having to wait for 60 days²⁸ if the subsequent request is refused earlier.

e) Confidentiality and user information

The EDPB notes that a specific Article²⁹ concerning the confidentiality of orders addressed has been introduced in the draft Regulation. In order to avoid any confusion and misunderstanding with the right to data protection, the EDPB recalls that although the GDPR provides that limitations to the rights of data subjects to safeguard the prevention, investigation, detection or prosecution of criminal penalties, should be provided by law and therefore publicly accessible³⁰ and that these legislative

²⁸ See Art. 10 (1)

²⁹ See Art. 11

³⁰ See Art. 23 (1) (d)

measures shall contain specific provisions as to the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction³¹, it does not provide for the obligation to inform individually data subjects of each access request made by law enforcement authorities.

However, in the meantime, the EDPB recalls that the Data protection directive provides for this right of information for the data subjects from the competent authorities themselves, unless this right has been limited, to any data subject without limiting this right only to data subjects residing in the territory of the EU.

f) Procedure for the enforcement of an order when the service provider refuses to execute it

The EDPB notes that Article 14 of the draft Regulation provides for a procedure to ensure the enforcement of an order when the addressee does not comply with it, relying on a judicial cooperation between the issuing authority and a competent authority in the enforcing State.

However, it appears that this procedure does not allow the enforcing authority to refuse to enforce the order transmitted on other grounds than purely procedural ones (the same as the addressee, mainly concerning the lack of information provided or the factual impossibility to provide the data), because the data concerned is protected by an immunity or privilege under its national law or because its disclosure may impact its fundamental interests such as national security and defence³².

The EDPB therefore reiterates its concerns as regards the removal of any double check by the receiving competent authority of the order transmitted, compared to the other instruments. Even the ground to refuse to enforce an order on the ground that it would violate the Charter appears higher than the classic threshold relating to a breach of the fundamental rights of the person concerned. Consequently, following the examples of the European Arrest Warrant, which provides for mandatory as well as optional grounds of refusal, or at least of the EIO Directive, which generally provides that the presumption according to which “the creation of an area of freedom, security and justice within the Union is based on mutual confidence and a presumption of compliance by other Member States with Union law and, in particular, with fundamental rights” is rebuttable³³, the draft Regulation should at least foresee the minimum classic derogation that if there are substantial grounds for believing that the enforcement of an Order would result in a breach of a fundamental right of the person concerned and that the executing State would disregard its obligations concerning the protection of fundamental rights recognised in the Charter, the enforcement of the order should be refused.

g) Enforcement of orders and conflicting obligations under third country laws (articles 15 – 16)

The EDPB welcomes the possibility provided in the draft Regulation for addressees to refuse an order on the ground that it would conflict with fundamental rights as it is aimed at providing safeguards in case of conflicting legal obligations. It also deems essential that the proposal provides for the consultation of third-countries authorities, at least where a conflict arises, as well as the obligation to lift the order when a third-country's authority raises an objection.

³¹ See Art. 23 (2) (h)

³² See Art. 14 (2)

³³ See recital 19 of the EIO Directive

Therefore, the procedure foreseen to refuse to execute an order on the ground of conflicting obligations under third country laws should be considerably improved.

First, the EDPB notes that the draft Regulation entrusts a private company, as addressee of a production order, to assess whether or not that order would be in conflict with applicable laws of a third country prohibiting the disclosure of the data requested. The company has to provide a reasoned objection including all relevant details of the law of the third country, its applicability to the case at hand and the nature of the conflicting obligations.

Most importantly, the EDPB is concerned that when such an objection is raised, the competent court of the Member State of the issuing authority alone assesses whether a conflict exists or not, since it is only when the court finds a conflict that it shall get in contact with the third country authorities. The competent EU court is therefore granted the competence to conclusively interpret the law of a third country in this context, without being that much of a specialist on the substance. The EDPB considers that the obligation to consult the competent authorities of the third country is therefore too limited in the current proposal. In the field of data protection, the EDPB draws the attention of the legislator to the fact that in case a competent court of a third country would interpret the GDPR to assess whether it is conflicting with its own requirements, the data protection authorities of the EU and the competent courts would remain competent to assess the legality of the transfer based on a judgment of a court or tribunal or on a decision of an administrative authority of a third country requiring a transfer or disclosure of personal data within the scope of the GDPR³⁴.

In addition, the EDPB underlines that the assessment of the law of the third country by the competent court of the EU requesting State needs to be based on objective elements, and is concerned by the criteria to be taken into account by the competent court when assessing the law of the third country under Article 15 (4) and 16 (5) (a) of the draft Regulation. Indeed, the Court would have to assess the fact that, “rather than being intended to protect fundamental rights or fundamental interests of the third country related to national security or defence”, the law of the third country “manifestly seeks to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations” or “the interest protected by the relevant law of the third country, including the third country’s interest in preventing disclosure of data”. For example, although in principle this assessment should require an evidence-based assessment in view of all available information given the potential impact of such a decision, at the very least, the wording (“is being aimed to”) appears unclear and should be adapted (“has the aim/objective to”).

The EDPB regrets that the only case where the authorities of a third country would be consulted and could object to the execution of a production order, would be where this competent EU court would consider that there is a relevant conflict, transmit all the elements to the central authorities in the third country concerned and the central authority of that third country would object within the tight deadlines of maximum 50 days (15 days, possibly extended by 30 days, and after a last possible reminder giving 5 additional days). In all other cases, the competent court would be in a position to uphold the production order and issue a pecuniary sanction of the service provider refusing to execute the order. Consequently, the EDPB is concerned that the competent EU courts will not have a wider obligation to consult the competent authorities of the concerned third countries in order to ensure that the procedure will more systematically ensure that the arguments of both sides will be taken into consideration and to show even more respect for the laws of third countries.

³⁴ See Art. 48 GDPR

As already underlined in the statement of WP29 and above, the EDPB recalls that particular attention should be paid to the adoption by third countries of similar instruments potentially affecting the rights of data subjects and their right to privacy within the EU, especially the risk of similar instruments that would enter in direct conflict with EU data protection law.

In addition, the EDPB underlines that the competent court of the Member State of the issuing authority may not even be the competent court to enforce the order foreseen under Article 14 of the draft Regulation, which would even increase the risk of conflicting procedures and the lack of counter-checks in a situation of conflicting laws. This comes from the fact that in some cases, three states could be involved: the one of the authority issuing the order, the third country of the service provider, and the Member State where the legal representative of the service provider in the EU is, and where the order would have to be enforced. Consequently, following the procedure currently foreseen, the court of the requesting authority in Member State A could make its own interpretation of the law of the third country B of the service provider without requiring the views of the authorities of this third country (while they would have objected to the order), and ask a court of another EU Member State C to enforce its decision without any possibility to object.

Besides, the EDPB also welcomes the introduction of specific remedies against production orders, in addition to remedies provided for in the GDPR and in the LED. The WP29 already called for such safeguards in its previous statement. However, the EDPB deplores that such remedies are not also foreseen against preservation orders, as these orders may also result in limitations of the fundamental rights of the individuals whose data are retained. Indeed, preservation orders may have the effect of retaining data for longer than they would have according to the data protection rules. Therefore, in itself, the preservation order results in a limitation of the fundamental rights of the concerned data subject, whose justification shall be subject to a review and to specific remedies, especially in cases where the preservation order will have been issued along with a production order to get the data. As recommended by the WP 29 in its statement, legal remedies, at least equivalent to those available in a domestic case should be foreseen.

h) Security of data transfers when responding to an order

The EDPB notes that the draft Regulation only provides for orders to be addressed to recipients within the European Union, and therefore does not provide for any specific channel for the transfer of data between the addressees and service providers located outside of the European Union.

Although the EDPB welcomes the absence of further derogations to the general framework of the EU for data protection, it recalls that any order sent to an addressee which would then imply a transfer outside the EU would need to respect the legal framework provided by the GDPR. Indeed, circumventing the legal framework of judicial cooperation, which provides for data protection safeguards to be respected, should not result as well in the circumvention of data transfer requirements by addressees of production or preservation orders to comply with such orders.

In addition, while the EDPB welcomes the absence of provision imposing an obligation to decrypt encrypted data³⁵, it is concerned that the draft proposals do not foresee any specific requirement for addressees to assess the authenticity of data produced and underlines that this assessment is also an added value of traditional instruments relying on judicial cooperation and warns against the increased risks posed for data subjects concerned in the absence of such an assessment.

³⁵ See recital 19 and page 240 of the impact assessment

Conclusions

Based on this assessment, the EDPB wishes to address the following recommendations to the co-legislators:

- 1) The legal basis of the Regulation should not be Article 82 (1) TFEU.
- 2) The necessity of a new instrument compared to the existing EIO Directive or MLAT should be better demonstrated, including with a detailed analysis of less intrusive means with regards to fundamental rights such as amendments of these existing instruments or the restriction of the scope of this instrument to preservation orders in combination with other existing procedures to request access to the data.
- 3) The Regulation should provide for a longer deadline to allow the executing service provider to ensure safeguards with regards to the protection of fundamental rights can be respected.
- 4) The dual criminality principle should be maintained, especially if the location criteria of the data is abandoned in order to maintain the obligation to take into consideration the safeguards provided in both concerned States (the State of the requesting authority and the State where the service provider is located).
- 5) The scope of the Regulation should be restricted to controllers in the sense of the GDPR or it should include a provision that in the event where the service provider addressed is not the controller of the data but the processor, the latter is obliged to inform the controller.
- 6) The Regulation should include safeguards concerning data transfers in case the service provider would be established in a third country without adequacy decision in this field or refer to the directive 2016/680 as these safeguards will be applicable.
- 7) Since the mandatory designation of a legal representative differs from the GDPR, the Regulation should precise that, the legal representative designated under the e-Evidence Regulation should be distinct from the one designated under article 3 (2) of the GDPR.
- 8) The Regulation should contain a broader definition of electronic communication data in order to ensure that the appropriate safeguards and conditions for access to be established cover both non-content and content data.
- 9) The Regulation should raise thresholds for issuing orders and orders shall be issued or authorised by courts, except for subscriber data provided the definition of this category of data is drastically narrowed to very basic information allowing only to identify a person without involving access to any communication data.
- 10) The Regulation should restrict the access to subscriber and access data to a list of crimes strictly established or at least to “serious criminal offenses”.
- 11) The time limit to provide data, especially in case of emergency should be better justified in the Regulation, and the possibility to use a fast 6-hour procedure should include the obligation for requesting authorities to demonstrate the emergency triggering the use of this procedure, even *a posteriori*, in order to allow for a control of the use of such exceptional powers.
- 12) The procedure allowing the production of content data without any involvement of the competent authorities of the Member State where the data subject is, should be abandoned.
- 13) Safeguards surrounding the issuing of European Preservation Orders should be improved in the Regulation.
- 14) The Regulation should at least include the minimum classic derogation that if there is substantial grounds for believing that the enforcement of an Order would result in a breach of a fundamental right of the person concerned leading the executing State to disregard its obligations concerning the protection of fundamental rights recognised in the Charter, the enforcement of the order should be refused.

- 15) The Regulation should foresee a broader obligation to consult the competent authorities of a third country where the service provider requested to provide data is located in case of conflict of laws in order to avoid subjective interpretations from a single court.
- 16) The validity and duration of preservation orders should be more linked to the production orders accompanying them.
- 17) The security of data transfers should be better guaranteed.
- 18) The verification of the authenticity of the data should be foreseen, in particular where encrypted data could be provided.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Guidelines



Guidelines 02/2022 on the application of Article 60 GDPR

Version 1.0

Adopted on 14 March 2022

EXECUTIVE SUMMARY

With the introduction of the GDPR, the concept of the one-stop shop was established as one of the main innovations. In cross-border processing cases, the supervisory authority in the Member State of the controller's or processor's main establishment is the authority leading the enforcement of the GDPR for the respective cross-border processing activities, in cooperation with all the authorities which may face the effects of the processing activities at stake: be it through the establishments of the controller or processor on their territory or through complaints from their residents against these processing activities. Indeed, data subjects should be able to easily pursue their data protection rights and should be able to complain to a supervisory authority at their place of habitual residence. This supervisory authority also remains the contact point for the complainant in the further course of the complaint-handling process. In order to meet all these requirements, Article 60 GDPR regulates the cooperation procedure between the lead supervisory authority and the other supervisory authorities concerned.

These guidelines handle the interactions of the supervisory authorities with each other, with the EDPB and with third parties under Article 60 GDPR. The aim is to analyse the cooperation procedure and to give guidance on the concrete application of the provisions.

General considerations

A common understanding of the terms and basic concepts is a prerequisite for the cooperation procedure to run as smoothly as possible.

Firstly, the guideline states that:

- the cooperation procedure applies in principle to all cross-border processing cases,
- the lead supervisory authority is primarily responsible for handling such cases, without being empowered to ultimately decide on its own, and that
- the cooperation procedure does not impact the independence of the supervisory authorities, which retain their own discretionary powers within the framework of cooperation.

It is recalled that the effects of national procedural regulations must not lead to limiting or hampering the cooperation under the GDPR.

Structure and Content of the guidelines

These guidelines are based on the requirements of Article 60 and clarify paragraph by paragraph the conditions arising from the regulation itself and its practical implementation.

In the context of Article 60(1) GDPR, it is established that the principles to be observed throughout the whole cooperation procedure are mutual obligations. It is stressed that while the achievement of consensus among the SAs is not an obligation, the endeavour to reach an agreed consensual decision is an overarching objective to be achieved through a mutual and consistent exchange of all relevant information. This exchange of information is obligatory for all CSAs, including the LSA. The meaning of "relevant" in this context is further clarified through examples. In terms of timeliness, the paper recommends sharing the relevant information proactively and as quickly as possible. Lastly, the possibility to use informal means of communication to reach consensus is recalled.

The following section on Article 60(2) GDPR addresses the situation of the LSA requesting CSA(s) to provide mutual assistance pursuant to Article 61 GDPR and conducting joint operations pursuant to Article 62 GDPR and provides guidance on the specifications of these instruments in the context of an ongoing cooperation procedure.

The paper addresses the process of the submission of the draft decision under Article 60(3) GDPR. It highlights that the LSA has to act proactively and as quickly as possible and that the CSAs should be able to contribute to the overall procedure, also before the creation of the draft decision (e.g. exchange of information). In addition, the LSA is required to submit a draft decision to the CSAs in all cases of cross border processing.

The sections on Article 60(4)-(6) GDPR outline the different scenarios that follow the submission of a draft decision by the lead supervisory authority and thus provide a consistent approach to the procedure between the submission of a (revised) draft decision and either the triggering of the binding effect in the absence of relevant and reasoned objections or the submission to the dispute resolution procedure. The guidelines also recognise the possibility for the LSA to adapt and resubmit the draft decision submitted under Article 60(4) GDPR prior to the expiry of the four-week period, provided that new factors or considerations justify such adaptation and that their importance is fairly balanced against the expediency of the cooperation procedure. In addition, it is specified that there may be multiple revised decisions but only in cases where it is likely to reach a consensus due to substantive convergence between the LSA and other CSA(s).

This is followed by the analysis of the different scenarios after the (revised) draft decision has become binding on the lead supervisory authority and the supervisory authorities concerned. It is clarified which supervisory authority has to adopt the final national decision pursuant to Article 60(7)-(9) GDPR on the basis of the draft decision that has become binding and which supervisory authority has to notify the controller/processor or the complainant. In this context, the distinction between notifying and informing is also addressed.

Furthermore, the guidelines address the important distinction between situations that constitute a dismissal/rejection of a complaint, with the consequence that the complaint-receiving SA adopts the final decision, and situations in which the lead supervisory authority acts on the complaint in relation to the controller, with the consequence that the lead supervisory authority adopts the final decision. In this context, it is highlighted that terms of EU law not making express reference to member state law must normally be given an autonomous and uniform interpretation.

The following section outlines the duties of the controller or processor to ensure that processing activities in all its establishments are in compliance with the final decision (Article 60(10) GDPR).

The last section addresses the specific requirements of the application of Article 66 GDPR (Urgency Procedure) in the course of an ongoing cooperation procedure (Article 60 (11) GDPR).

A quick reference guide annexed to the guidelines is intended to give practitioners in the supervisory authorities a quick overview of the procedure and to illustrate the complex procedure.

Table of contents

EXECUTIVE SUMMARY	2
1 Introduction	6
2 Article 60 in the framework of the OSS-system.....	7
2.1 Applicability of the cooperation procedure.....	7
2.2 LSA/CSA as involved actors.....	8
2.3 Independence of SAs within the cooperation procedure	10
2.4 Impact of national procedural rules	11
3 Article 60(1) – mutual obligation.....	11
3.1 General	11
3.2 The endeavour to reach consensus	12
3.3 The obligation to exchange all relevant information	12
3.3.1 The term “Relevant information”	13
3.3.2 Timing of the information exchange.....	14
4 Article 60(2) – mutual assistance and joint operations	15
4.1 General	15
4.2 Requirements of Article 60(2)	15
4.2.1 The LSA may request	16
4.2.2 The term “At any time”.....	16
4.2.3 The other CSAs as addressees	16
4.3 Requests for mutual assistance	17
4.4 Setting up joint operations	18
5 Article 60(3) – Information by the LSA and draft decision obligation.....	18
5.1 Article 60(3)(1): LSA’s obligation to share information without delay.....	18
5.1.1 The term of “without delay”	18
5.1.2 The term of “relevant information”	19
5.2 Article 60(3)(2): LSA’s obligation to issue a “Draft Decision”	21
5.2.1 Legal obligation to submit a draft decision	21
5.2.2 The term of “draft decision”	22
5.2.3 The term of “without delay” regarding the submission of the draft decision	24
5.2.4 The term of “taking due account of their views”	25
6 Article 60(4) – Assessment of the objections and possibility to trigger a dispute resolution process	26
6.1 Purpose of the provision	26
6.2 Relevant and reasoned objections by a CSA.....	27

6.2.1	Calculation of the deadline	27
6.2.2	Relevant and reasoned objections.....	28
6.2.3	Assessment of the objections to the draft submitted under Article 60(4).....	29
6.3	Submission to Board.....	30
7	Article 60(5) - The Revised Draft Decision	31
7.1	Submission to the other CSAs.....	31
7.1.1	The LSA intends to follow	31
7.1.2	The obligation to submit a revised draft decision.....	31
7.1.3	The submission of the revised draft decision	32
7.1.4	The views of the other CSAs	33
7.2	The Revised Draft Decision: Assessment Procedure.....	34
7.2.1	Joint application of Article 60(5) second sentence and the procedure of Article 60(4)	34
7.2.2	Constraints on other CSAs in submitting relevant and reasoned objections to the revised draft decision	35
8	The binding effect of a (revised) Draft Decision	36
8.1	Deemed to be in agreement with the draft decision.....	36
8.2	Bound by the draft decision	36
9	Article 60(7) – the LSA adopting and notifying the decision.....	37
9.1	General	37
9.2	Adoption of the final decision by the LSA	38
9.3	Notification and information	39
9.4	A summary of the relevant facts and grounds.....	40
10	Article 60(8) –The dismissal/rejection of a complaint	40
10.1	Derogation from paragraph 7.....	41
10.2	The term “Dismissal/Rejection”	41
10.3	Adoption of the decision	44
10.4	Inform and notify.....	45
11	Article 60(9) – partial dismissal/rejection.....	45
12	Article 60(10) – notification of the measures adopted by the controller or processor to the LSA/CSA(s).....	46
13	Article 60(11) – urgency procedure	47
13.1	The conditions for invoking Article 66	47
13.2	The interaction with an ongoing Article 60 cooperation procedure.....	48
	Quick Reference Guide.....	50

The European Data Protection Board

Having regard to Article 70(1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

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

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. The number of national enforcement proceedings concerning cross-border data processing activities is constantly increasing, with many being resolved within the GDPR cooperation mechanism. While Article 57(1)(g), (f) set the frame for the general cooperation, the One Stop Shop (OSS) is established under Article 56 and 60 GDPR². This specific procedure requires the Lead Supervisory Authority (LSA) to cooperate with the other Concerned Supervisory Authorities (other CSAs) in an endeavour to reach consensus.
2. It should be underlined that the OSS model, allowing the supervisory authorities (SAs) of all Member States (MS) to be involved in a type of co-decision procedure, is a novel concept to data protection legislation introduced by the GDPR.
3. These guidelines handle the interactions of the SAs with each other, with the EDPB and with third parties under Article 60. The aim is to analyse and give guidance on the concrete application of the provisions. As the cooperation procedure relates to processing activities, its outcome concerns, by definition, the actors involved in such processing (data subject, controller, processor(s), etc.). However, since the duty to cooperate contained in Article 60 applies to SAs, this paper focuses on the obligations of the LSA and other CSA(s).
4. It is, not in the scope of these guidelines to address the issue of designation of the LSA and other CSAs. These guidelines presume that this has been clarified and agreed according to Article 56 as the Article 60 procedure attributes specific competences and actions to the involved SAs based on their roles. Therefore, it is assumed that sufficient information to establish the different roles has been already shared at the point that the work under Article 60 GDPR starts.

¹ References to “Member States” made throughout these Guidelines should be understood as references to “EEA Member States”.

² The term “Article” without further specification refers to those of the GDPR.

5. However, in specific situations there might occur later on a shift in the competences and roles of the SAs (e.g. a new location of the main establishment or a case of joint controllership). Therefore, as soon as the SAs get knowledge of any circumstance that might affect the competence for handling the case during the cooperation phase, information should be shared immediately among SAs, in order to identify the new presumed LSA and to reach an agreement on the allocation of roles³.
6. Upon agreement, the Article 60 procedure would proceed accordingly. If consensus cannot be achieved, the matter is to be referred to the EDPB making use of Article 65(1)(b).
7. Whenever in these Guidelines reference is made to the use of the "*EDPB Information System*", such reference means the Internal Market Information System ("IMI") in pursuant to Regulation (No) 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation using the Internal Market Information System and repealing Commission Decision 2008/49/EC ("IMI Regulation")⁴. The EDPB Information System shall be used in accordance with Article 60(12) for the supply of all information required under Article 60. In addition, SAs should use all forms of communication, such as e-mails, phone, videoconference or in person, to facilitate the process of achieving consensus.

2 ARTICLE 60 IN THE FRAMEWORK OF THE OSS-SYSTEM

2.1 Applicability of the cooperation procedure

8. The cooperation procedure between the LSA and the other CSAs under Article 56(1) and Article 60 essentially has the following conditions: the processing operation has to be cross-border according to Article 4(23), which also means that the controller or processor must have a main or single establishment in the EU. Article 4(23) provides for two alternative connected definitions. Firstly, Article 4(23)(a) requires that the controller or processor has establishments in more than one MS. Secondly, the specific data processing operation in question has to be carried out in the context of the activities of several EU establishments. According to Article 4(23)(b) the effects on data subjects can define cross-border processing. In case the processing takes place in the context of the activities of a single establishment of a controller or processor within the EU, cross-border processing is assumed if the processing substantially affects or is likely to substantially affect data subjects in more than one MS.⁵
9. The EDPB stresses that Articles 56 and 60⁶ apply to the cooperation between SAs in all cases based on cross-border processing, without regard to the origin of the case (complaint, ex officio inquiry, etc.). This is without prejudice to the provisions of Article 55⁷ and Article 65.
10. While only Article 60(7) last sentence as well as paragraphs 8 and 9 refer to the handling of complaints, Article 56(1) and Article 60 as the core provisions concerning the cooperation procedure refer to cross-border processing in general. With regard to the cooperation mechanism, Article 60(3) also refers to the fact that the LSA shall "*communicate the relevant information on the matter*", i.e. the case in

³ See also: Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment

⁴ See Also Article 17 of the Rules of Procedure of the EDPB.

⁵ See also: WP244 Guidelines for identifying a controller or processor's lead supervisory authority.

⁶ Except in the case described in para. 13 below.

⁷ See also: Recital 128.

general, so that it is not at all limited to complaint-based cases. The term “*matter*” includes for instance “*ex officio*” proceedings and the possibility under Article 57(1)(h) to conduct an investigation e.g. on the basis of information from another SA or other public authority. As complaint handling is already covered by Article 57(1)(f), this information provided according to Article 57(1)(h) does not have to be based on a complaint.

11. Furthermore, this is supported by a systematic approach with regard to possible sanctions or remedies under Article 58(2), which applies to all types of processing and not just to complaints.

Example 1: Sources originating from the media or from whistle-blowers provided by a CSA may also initiate an Article 60 procedure if they are specific and substantial, i.e. facts are presented in a concrete and complete manner. However, simply forwarding a newspaper article without more detailed information, e.g. an initial evaluation by the CSA, does not regularly constitute sufficient evidence of a data protection breach and would therefore not be considered to be sufficiently substantiated to cause supervisory measures. On the contrary, firm evidence does not need to be provided to open an Article 60 procedure, because the procedure itself aims to establish whether an infringement exists or not. However, the LSA has wide discretionary powers to decide when to initiate an investigation *ex officio* based on information received on potential infringements from other CSAs or sources.

12. The application in all cross-border cases also follows from the purpose of the cooperation mechanism: It was created “*to foster a uniform application of the data protection rules through a consistent interpretation*”⁸ and to ensure effective supervision and enforcement within the Union. A limitation to complaint-based cases would contradict this purpose.
13. For cases with only local impacts, Article 56(2) and 56(3) provide that the SA, which received the complaint or was made aware of a possible infringement, shall be competent if the LSA decides not to handle the case. Article 60 does not apply in these cases. Only where the LSA decides to handle the case Article 60 is applicable according to Article 56(4).

2.2 LSA/CSA as involved actors

14. Article 56(1) contains a legal definition of the competent LSA; that definition is to be read in conjunction with Article 60, which sets out the essential tasks and powers of the LSA in the Article 60 procedure⁹. The LSA is defined as the SA of the main establishment or of the single establishment of the controller or processor in the Union, which is competent for the cross-border processing carried out by that controller, or processor. It is also the sole interlocutor for that controller or processor according to Article 56(6).
15. The relevant starting point for determining the LSA is the specific cross-border processing of data (“carried out”) by the respective controller or the processor¹⁰.
16. WP244 clarifies that “*a lead supervisory authority is the authority with the primary responsibility for dealing with a cross-border data processing activity*”. In other words, the LSA has the competence for the cross-border processing carried out by the given controller or processor, being the sole interlocutor

⁸ COM (2020)264 final, p.6.

⁹ For “*local cases*” under Article 56(2), the provisions of Article 56(3) and (4) must be observed.

¹⁰ For further information on this matter see also: WP244 rev.01: “Guidelines for identifying a controller or processor’s lead supervisory authority”

for that controller or processor in the respective MS under Article 56(6). Within the framework of the cooperation procedure set out in Article 60, and pursuant to Article 56(1), this competence translates into a ‘leading function’, i.e. into a steering role in taking the case forward, organising the cooperation procedure with a view to involving the other CSAs, coordinating investigations, gathering evidence etc. as well as in the responsibility for submitting a draft decision which is subject to opinions or objections by the other CSAs¹¹.

17. However, the EDPB considers the LSA not to have exclusive competences with regard to the cooperation process, i.e. the GDPR provides for a shared responsibility to monitor and enforce the application of the GDPR in a consistent manner, so that the LSA's position is subject to the views of the other CSAs and the outcome should be a consensually reached decision. This is made clear by the decision of the Union legislator that in cases of persistent disagreements between SAs, these must be resolved by the EDPB pursuant to Article 65(1)(a).
18. According to Article 4(22) a CSA means a SA which is concerned by the processing of personal data because:
 - (a) the controller or processor is established on the territory of the MS of that SA¹²;
 - (b) data subjects residing in the MS of that SA are substantially affected or likely to be substantially affected by the processing; or
 - (c) a complaint has been lodged with that SA.
19. The EDPB considers these requirements to be basically obvious and simple to state so that, in principle, no special requirements need to be observed here. In terms of factor (a), the existence of an establishment will generally be easy to determine. The same applies to (c) and the question whether a particular SA has received a complaint. It is to be noted that in (b) the data subject must merely reside in the MS in question; he or she does not have to be a citizen of that state¹³.
20. In the event of doubt, it seems appropriate with regard to the legal consequences that basically each authority needs to substantiate its reasoning for being concerned.
21. The term "*substantially affected*" has been further defined in WP244 by naming factors (such as use of a particular language, use of a particular currency, availability of a service in the MS concerned, concrete address through controller or processor etc.) which shall be taken into consideration by each authority when assessing whether they are concerned.
22. When at any point a previously non-concerned SA becomes concerned during an ongoing Article 60 procedure (for instance by receiving a complaint), the following basic procedure can be envisaged:
 - The CSA should immediately notify the LSA of its status and request its inclusion into the OSS procedure.

¹¹ In this respect the role of the LSA has been characterised as at several points “*primus inter pares*”, e.g. by the Advocate General in his Opinion on Case 645/19, para. 111.

¹² For further information in the context of the term “*establishment*” see EDPB Guidelines 3/2018, p.5-7 as well as regarding the term of “in the context of the activities of an establishment” 3/2018 p.7-9.

¹³ See also: WP244 Guidelines for identifying a controller or processor’s lead supervisory authority, p.9.

- The LSA should make sure to involve this new CSA as such, especially in the respective case register, and should inform the new CSA of its inclusion into the decision-making procedure. If the LSA becomes aware that a not yet involved authority is or has become a CSA, it should inform it about this change of status¹⁴.
23. The involvement of a newly concerned SA in an ongoing cooperation procedure should be possible at any stage of the case but cannot have any effect on the procedure enshrined in Article 60. As a result, all deadlines and procedures prescribed by Article 60 remain unaffected, i.e. for instance the deadline of Article 60(4), once the LSA has submitted its draft decision, applies irrespective of the fact that in the meantime a new CSA could join the procedure.
24. For this reason, the CSA may consider whether its respective case can still be handled effectively within the ongoing cooperation procedure and whether it should rather open a new procedure, for instance because the current one does not cover (some) core issues in the case before the CSA.

2.3 Independence of SAs within the cooperation procedure

25. Within the cooperation procedure, both the LSA and the other CSAs act as independent SAs according to Article 52(1).
26. However, the CJEU stressed¹⁵ that the independence of the SAs was introduced in order to give greater protection to the data subjects concerned and not to confer a special status on the supervisory bodies themselves¹⁶. Independence is therefore to be understood as absolute protection against any external influence. However, in this context, the SAs form a unit within the framework of a European administrative network, within which they are responsible for ensuring the consistent application of the GDPR throughout the Union.
27. The reference to the cooperation procedure in the provision establishing the SAs (Article 51(2)) underlines the importance of the cooperation mechanism for the functioning of a unified supervision and an effective protective standard through a consistent application of the GDPR within the Union.
28. In this respect, the EDPB underlines that all steps within the cooperation procedure are compatible with the legally prescribed independence granted to SAs pursuant to primary law and Article 52, as such independence is from external influence as clarified above and has no bearing on the general obligation to cooperate that is set out as an overarching duty within Article 60.
29. It should be noted that SAs, as national administrative authorities, enjoy a certain margin of discretion pursuant to domestic law in deciding with all due diligence the course of action that can best achieve the public interest they serve (see Article 51(1)). This discretionary power must be exercised in line with the provisions of the GDPR and in accordance with appropriate procedural safeguards set out in Union and Member State Law, impartially, fairly and within a reasonable time.
30. Thus, the discretion to be acknowledged to SAs acting as independent administrative authorities, free from the influence of external stakeholders, cannot be unlimited in particular vis-à-vis EU law, as they

¹⁴ The whole process should be conducted by using the EDPB information system.

¹⁵ CJEU Case C-518/07, *Commission v Germany*, para. 25 and 32 et seq. [ECLI:EU:C:2010:125], Case C-362/14, *Schrems v DPC*, paras. 99 [ECLI:EU:C:2015:650]; confirmed in Case – C-311/18, *Schrems II* para. 115 [ECLI:EU:C:2020:559].

¹⁶ Case C-518/07, para. 25 [ECLI:EU:C:2010:125], see also Case C-362/14, para. 41.

(both the LSA and the other CSAs) are required to act cooperatively and are accountable for their decisions (or non-decisions) regarding a given case.

2.4 Impact of national procedural rules

31. Since the GDPR does not regulate all details of cooperation, the tasks and powers entrusted to SAs by Article 57 and Article 58 have to be fulfilled by relying on national procedural law.
32. It is usual that EU legal instruments may include procedural provisions (such as the GDPR Articles conferring certain powers on SAs), but insofar as EU law does not provide for specific procedural rules, national procedural law applies. In these cases the principle of national procedural autonomy, which is a general principle of EU law, generally applies. This general principle is limited, as is outlined extensively in the case law of the CJEU, by the EU principles of equivalence and effectiveness¹⁷. These principles stipulate that the applicable national rules must not treat an EU determined matter more unfavorably than purely national ones (equivalence). In addition, the application of national provisions must not significantly complicate or make it practically impossible to realise the purpose of the European legal standards (effectiveness).
33. However, since such different national administrative rules exist, their application may lead to differences and may (partly) be the reason why SAs handle cases in different ways and investigate them differently. Nevertheless, these distinctions in national (procedural) law must not lead to situations in which the principles of equivalence and effectiveness are undermined.
34. Accordingly, if it is not possible to reconcile EU law and national requirements in this way, i.e. if the national provision contradicts EU law, the national regulations that contradict EU law must in principle remain unapplied¹⁸.
35. Regarding the cooperation mechanism the EDPB stresses therefore that national (procedural) law having impact to the effect of '*significantly complicating or making it practically impossible to realise*' effective cooperation is not compatible with the GDPR and '*must be reconciled with the requirement of uniform application of Community law so as to avoid unequal treatment*' (ECJ, C-290/91, para. 8). This being an obligation imposed on all Member States, if the above reconciliation proves impossible, the consequence is that an authority should consider not applying such national law.

3 ARTICLE 60(1) – MUTUAL OBLIGATION

3.1 General

36. Article 60(1) provides for a general duty of cooperation, which obliges all involved SAs equally. The wording clarifies by the use of "*shall*" that the obligation to cooperate is not a matter of discretion but a legal obligation.
37. Article 60(1) lays down basic and overarching principles, which apply throughout the entire cooperation between SAs. In accordance with the wording of this Article, the key concepts of the

¹⁷ Regarding the OSS see: Case 645/19 para. 53: '*The application of the ‘one-stop shop’ mechanism consequently requires, as confirmed in recital 13 of Regulation 2016/679, sincere and effective cooperation between the lead supervisory authority and the other supervisory authorities concerned.*'

¹⁸ See also: CJEU: Case C-205-215/83, para. 19; C-94/87, para. 12; C-280/13, para. 37.

cooperation procedure consist of “*an endeavour to reach consensus*” and the obligation to “*exchange all relevant information*”.

38. The EDPB expressly points out that these obligations are to be complied with by the LSA and every other CSA (mutual obligation).

3.2 The endeavour to reach consensus

39. The “*endeavour to reach consensus*” is to be understood as a legal objective¹⁹, which does not lead to a legal obligation to reach consensus in a respective case. However, this legal objective has a decisive influence on all actions of all CSAs throughout the entire cooperation process, i.e. it sets the direction for cooperative acting in such a way that SAs do their utmost and make a “*serious determined effort*”²⁰ in order to achieve consensus.
40. The cooperation procedure conducted in an “*endeavour to reach consensus*” necessarily entails a mutual exchange of views and documents on the subject matter. This mutual exchange is intended to ensure that all circumstances relevant to the case have been taken into account and could thus also contribute to prevent disputes²¹.
41. That consensual acting should be the rule is further illustrated by the provisions contained in Article 60(11) and Article 66(1) whereby “*in exceptional circumstances*” and “*by derogation to (...) the procedure referred to in Article 60*”, respectively, a CSA may take urgent measures²².
42. The importance of this objective is confirmed by the comparison between the current text and the original 2012 Commission proposal for the GDPR, which did not mention “*consensus*” and envisaged simply the exclusive competence of the LSA in cross-border cases. The current text mirrors a different approach endorsed by the EU legislator, where emphasis is placed on the mandatory cooperation of the SAs, which is supposed to be fair and constructive²³. In their efforts to reach consensus, SAs should use all possible tools, including mutual exchanges of relevant information, providing each other with an opportunity to express their views on exchanged information and take into account the point of view of other CSAs²⁴.
43. As a result, this translates into a mutual obligation placed on the LSA and other CSAs to select cooperation approaches that are best suited to achieve consensus as described.

3.3 The obligation to exchange all relevant information

A key as well as further priority element of the cooperation procedure lies in the mandatory (“*shall*”) exchange of “*all relevant information*” between the involved SAs – this applies throughout the whole cooperation procedure.

¹⁹ See also: Case C-645/19 para. 51 ‘...the lead supervisory authority is, in particular, required to endeavour to reach consensus.’

²⁰ Merriam-Webster: “endeavour”.

²¹ See also: Guidelines 9/2020 on relevant and reasoned objection under Regulation 2016/679, para. 9.

²² See also: Recital 138 stating that “*in other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied (...) without triggering the consistency mechanism*”.

²³ See also: Opinion of AG on Case C-645/19, para. 87.

²⁴ 2012/0011 (COD) Article 51(2).

44. The exchange of relevant information is a mutual obligation that is necessary to enable the LSA and the other CSAs to effectively fulfil their roles e.g. when determining whether there has been an infringement of the GDPR²⁵.
45. The mutual exchange of information is particularly important if no joint operations (Articles 60(2), 62) are envisaged by the LSA and no mutual assistance requests (Articles 60(2), 61) are relied upon to jointly gather relevant information. Without these additional procedures, which naturally require further engagement and coordination, the LSA and other CSAs have to rely on the mutual exchange of information as per Article 60(1)(2).

3.3.1 The term “Relevant information”

46. Which information is to be considered as “relevant” depends on the circumstances of each individual case. In principle, all information that is directly or indirectly conducive to the conclusion of the proceeding should be classified as relevant. This includes sufficient information about the factual elements and legal issues specific to the case. Information that is already known or publicly available does not necessarily need to be shared.
47. The exchange of information is therefore not an end in itself, but serves all SAs involved to deal with the case and to be able to fulfil their role as SAs properly. For practical implementation, it is therefore imperative that all parties involved act appropriately, i.e. proportionately and in the spirit of good cooperation. Therefore, the question in each case should be basically what information every SA would necessarily need itself in order to deal with the case.
48. For instance, in the case of a LSA, this refers to all relevant information gathered in dealing with the controller or processor – the LSA being “*the sole interlocutor*” of the controller (findings of investigations, reports, exchanges with the controller, records of meetings, further evidence etc.).
49. If the information is especially substantial in amount and scope the LSA should find ways to provide summaries, extracts, reports to substantiate the arguments made in the draft decision.
50. In the case of another CSA, this should translate into an obligation to proactively disclose, to the LSA as well as the other CSAs, all the relevant information regarding the case (complaint, data breach notification etc.) of which that SA is in possession and that is helpful in assessing the legal and factual situation of the case. This may include any pleadings, arguments, correspondence with data subjects or any findings made by the CSA in the course of e.g. the vetting phase, or national inspections that have led to the detection of a possible infringement at the national establishment of the controller in a cross-border context.

For instance, the following information could be exchanged between the SAs:

- Information that has consequences for the reallocation of the competences of the LSA and the distribution of roles/qualification of CSAs²⁶ (e.g. change in controllership or main establishment, etc.)
- Correspondence with data controller/data subjects on the subject of a complaint or investigation

²⁵ See also: EDPB, Decision 01/2020 on the dispute arisen under Article 65(1)(a) GDPR, at para. 134-136.

²⁶ See para. 5 above.

- Meetings with controllers or processors: Agenda, scope and task, minutes of the meeting/assessment of the outcome of the meeting, intended follow up actions
- Minutes of hearings and rehearsals – also related to single issues of the case
- Questionnaires sent to the controller/processor
- Possible first draft report of the investigation/inspection
- Possible Expert reports (legal, technical) also from external providers
- Intended scope of an investigation/Inspection report/minutes of investigations
- Witness statements and other legal evidence, other relevant indications, experience in relation to the controller or processor or the data processing, administrative practice
- Information required to set the right focus: for instance, for an investigation into a very technical subject matter, it is likely that information relating to the technical aspects is very relevant, where in other cases the technical aspects are less relevant
- Note: The examples given above are non-exhaustive. Which information will be deemed by SAs to be relevant information will depend on the circumstances of the specific case.

For exchange of such information, the EDPB Information system should be used.

51. With regard to the data minimisation principle of Article 5(1)(c), it should be assessed case by case whether the communication of personal data is necessary. Personal data should be shared only if required to deal with a specific issue.
52. The LSA and other CSAs may flag specific pieces of information as (highly) confidential, particularly when this seems necessary in order to meet requirements of confidentiality constraints laid down in national laws. In such a case, the SAs should inform each other immediately and jointly find legal options for a solution against the background that confidentiality provisions usually relate to external third parties and not to CSAs. In this regard, any information received that is subject to national secrecy rules should not be published or released to third parties without prior consultation with the originating authority, whenever possible.
53. As regards requests for public access, without prejudice to national transparency regulations, SAs should consult each other before granting or refusing access to documents, which were exchanged during the cooperation procedure.

3.3.2 Timing of the information exchange

54. No specific timeline is provided in paragraph 1, as this is a general obligation irrespective of the timing involved. However, effective enforcement of the GDPR throughout the EU requires that all CSAs receive all relevant information in a timely manner, i.e. as soon as reasonably possible. Therefore, the EDPB considers the mutual obligation to exchange all relevant information necessarily to apply already prior to the submission of a draft decision by the LSA.
55. In order to facilitate the reaching of consensus, the information should be shared at a moment where it is still possible for the LSA to take on board the viewpoints of the other CSAs. This should apply to any stage of the proceedings, and in particular, it should prevent the other CSAs from being presented

with accomplished facts, for example because certain stages of the proceedings may be precluded under national law.

56. In this respect, Article 60 provides also ‘space for thought’ to both LSA and other CSAs in that there is room for facilitating the achievement of consensus through ‘informal’ exchanges of “*all relevant information*” without strict deadlines prior to triggering the ‘formal’ steps. The more comprehensive and timely the exchange of information between the SAs involved, the greater the likelihood of reaching a consensus as early as possible will be.
57. The EDPB recommends therefore as a minimum standard that the LSA makes all efforts to proactively share, with the other CSAs, the scope and main conclusions of its draft decision prior to the formal submission of the latter. This enables the other CSAs to form their own views in that respect and timely flag possible questions to the LSA. The LSA may decide to address these issues prior to issuing the draft decision formally and thus before triggering the very strict procedure envisaged in Article 60(4) and 60(5) for raising objections to the draft decision.
58. After all, it should be kept in mind that the cooperation mechanism is intended to be supportive and serve the effective enforcement of data protection within the EU. SAs will need to develop best practices through the continuous gathering of practical experience by being flexible in choosing optimal ways for cooperation.

4 ARTICLE 60(2) – MUTUAL ASSISTANCE AND JOINT OPERATIONS

4.1 General

59. Article 60(2) addresses specific forms of cooperation between the LSA and the other CSAs throughout the cooperation procedure provided for by Article 60, i.e. within the framework of the OSS mechanism.
60. Article 60(2) goes beyond the duty to exchange all relevant information, provided for by Article 60(1), and provides for a specific kind of cooperation that the LSA may pursue if necessary in a concrete case: either requesting CSA(s) to provide mutual assistance or requesting CSA(s) to engage into a joint operation conducted by the LSA.
61. The application of Articles 61 and 62 in the remit of Article 60(2) entails reading the provisions of those articles in conjunction with Article 60, and, therefore, they have to be adjusted to the precise context of a cooperation procedure and to the allocation of roles provided by the OSS mechanism, and in particular provided by Article 60(2).
62. By specifying the main purposes of such cooperation, i.e. for carrying out investigations or for monitoring the implementation of a measure concerning a controller or a processor in another MS, Article 60(2) emphasises two stages of the cooperation procedure where those cooperation tools are applicable: firstly, during the investigatory phase, before the final decision is adopted ; secondly, during the implementation phase, after the final decision was adopted and notified to the controller or processor.

4.2 Requirements of Article 60(2)

4.2.1 The LSA may request

63. By referring to the LSA, this provision frames the action to be taken within the OSS mechanism while placing it within a specific case being handled, after the LSA has been identified. It should then be stressed that the possible resort to mutual assistance or to joint investigations pursuant to Article 60(2) is limited to the cooperation procedure related to the specific ongoing cross-border case.
64. Following the LSA's level of discretion to conduct the investigation or to follow-up the measures taken by the controller or processor to comply with its decision, the wording "*may request*" empowers the LSA to take the initiative, but only if it deems necessary or appropriate for the case at hand. It is up to the LSA to decide whether to make a request for mutual assistance or to have a joint operation, pursuant to Articles 61 and 62 respectively, as the GDPR does not impose on the LSA an obligation to use such possibilities.
65. Article 60(2) only covers requests made by the LSA, and not requests from the CSA²⁷ addressed to the LSA in the context of the Article 60 cooperation procedure, as those are already envisaged by Article 60(1) under the "*exchange of relevant information*".

4.2.2 The term "At any time"

66. This means that the LSA may send requests for mutual assistance or for a joint operation, whenever the LSA considers the action justified to fully exercise its competence throughout the cooperation procedure provided for Article 60.
67. Indeed, within the same cooperation procedure, related to a specific case, the LSA may send several different requests, related to mutual assistance or to a joint operation or both. The LSA should bear in mind though that such requests should be necessary and adequate for the investigation and decision-making process or for monitoring the implementation by the controller or processor of the LSA's decision.

4.2.3 The other CSAs as addressees

68. According to Article 60(2), the addressees of the requests by the LSA are in general the other CSAs, which have actively expressed to be concerned in the specific cooperation procedure²⁸. In case of Article 61 mutual assistance requests, this does not imply that all CSAs are automatically addressees of the requests or have to be involved in the action at stake. That would depend on the assessment of the LSA on who is in the best position to contribute to the ongoing case. Conversely, when the LSA intends to carry out joint operations, all of the relevant CSAs have the right to participate pursuant to Article 62(2)²⁹.
69. In the last phase of the cooperation procedure, provided for in Article 60(10), which relates to the follow-up of the compliance of the LSA's final decision by the controller or processor, again the LSA may decide, based on the specifics of the case at hand, which CSA(s) are to be involved in actions

²⁷ Pursuant to Article 56(5), whenever the LSA decides not to handle the case in view of its local nature, the CSA assumes then the leading role of the investigation and shall handle it according to Articles 61 and 62. If it happens that the CSA handling the case may need to request assistance to the LSA, Article 60 procedure does not apply, so Articles 61 and 62 will be directly applicable outside the scope of Article 60(2).

²⁸ See para. 36189 et seq. on the binding effect of the draft decision.

²⁹ However, the LSA is at liberty to extend the participation to SAs that are not CSAs.

intended to verify *on the spot* the implementation of the decision and it will send the assistance requests accordingly (e.g. the CSAs of the MS where the controller or processor have establishments).

4.3 Requests for mutual assistance

70. The mutual assistance instrument comprises a variety of possibilities for SAs to cooperate with each other, in order to implement and apply the GDPR in a consistent manner, taking into account the geographical dispersion of data controllers' or processors' establishments and of data subjects. However, the specific type of assistance requested will depend on the specific circumstances of the case, also taking into account that the LSA is the sole interlocutor of the controller or processor for the specific cross-border processing case being handled.
71. In a cross-border case within the Article 60 procedure, the LSA can send to the CSA(s) a request for any type of mutual assistance that is considered to be helpful for reaching a decision in the specific case.
72. During the investigatory phase, there are several situations where the LSA may need to request mutual assistance from other CSA(s). The most common one may be the case to ask for assistance of the CSA where the complaint was lodged (e.g. to seek for additional information to be provided by the complainant; to have certain facts checked or evidence collected in the organisation establishment of that MS). In such situations, only one CSA would be involved.
73. However, the LSA may need to request the CSA(s) to provide information or to carry out an investigation in specific establishment(s) of the controller or processor in some MS, in view of the conditions under which the data is being processed or the partition of responsibilities among establishments. In these circumstances, the LSA will address the request to the relevant CSA(s).
74. At the end of the Article 60 procedure, after the controller or processor has notified the LSA on the measures taken to comply with the LSA's final decision, as per Article 60(10), the LSA, upon information on that fact to the other CSA(s), may still request the CSA(s) to provide mutual assistance, in the form of verification, if – and how – the establishment of that controller or processor in that MS implemented the decision.
75. The mutual assistance requests sent under Article 60(2) should follow the general rules of Article 61, in what regards the purposes and reasons substantiating the request by the LSA on one hand, and the possible reply by the CSA(s) on the other.
76. In accordance with Article 61(2), when receiving a request by the LSA, the CSA(s) shall take the appropriate steps to reply "*without undue delay*", and in any case "*no later than one month after receiving the request*".
77. The principle of giving priority, to a certain extent, to the Article 60 procedure is already enshrined in Article 60(3) where the term "*without delay*" is used, as well as in the strict deadlines provided for in paragraphs 4 and 5. The term "*undue delay*", used in Article 61, also stresses the need for the SA to act promptly, though the variety of actions covered by the mutual assistance requests may imply different timelines to fully give satisfaction to a request. In any way, the CSA(s) shall inform the LSA no later than one month after receiving the request "*of the results or, as the case may be of the progress of the measures taken to respond to the request*," as per Article 61(2) in conjunction with Article 61(5).

4.4 Setting up joint operations

78. In accordance with Article 60(2), the LSA may conduct joint operations pursuant to Article 62, in particular to carry out investigations or to monitor the implementation of a measure concerning a controller or processor established in another MS.
79. Therefore, within the LSA's leading role in the Article 60 procedure, whenever it considers that the ongoing case benefits from a joint investigation or from joint enforcement measures, the LSA may set up a joint operation by requesting the CSA(s) to engage in such action, though there is no obligation for a CSA to reply positively.
80. A joint operation can be hosted by the LSA in its MS or it could be organized by the LSA as a joint investigation action of the CSAs to be deployed in several MS, where there are establishments of the controller or processor, to make verifications on the spot necessary for the outcome of the cooperation procedure. A joint operation can also be triggered by the LSA, as a joint enforcement measure of the relevant CSAs to monitor simultaneously the implementation of the LSA's decision in each establishment of the controller or processor upon which the decision is binding.

5 ARTICLE 60(3) – INFORMATION BY THE LSA AND DRAFT DECISION OBLIGATION

81. Article 60(3) describes the decision-making process, which is a key step in the cooperation procedure between the LSA and the CSAs. The aim of this phase is to quickly find a consensus decision concerning the outcome of the case.
82. Article 60(3) focuses on the duties of the LSA and establishes three key obligations:
 - communication of the relevant information on the matter to the CSAs without delay,
 - submission of a draft decision to the other CSAs for their opinion without delay, and
 - taking due account of the CSAs' views.

These obligations are to be regarded in line with the consensual approach established in Article 60(1).

5.1 Article 60(3)(1): LSA's obligation to share information without delay

5.1.1 The term of "without delay"

83. The term "*without delay*" is used in both sentences of Article 60(3). While sentence 1 contains the obligation of the LSA to communicate without delay the relevant information on the matter to the other CSAs, sentence 2 stipulates the LSA's obligation to submit without delay a draft decision to the CSAs.
84. Although the term "*without delay*" is used in various places in the GDPR, it is not further defined in Article 4.
85. Since Article 60(3) is a legal provision under Union law, the term "*without delay*" must be interpreted autonomously from national law to ensure a uniform application of the GDPR.
86. The term "*without delay*" was subject of the judgement of the CJEU (18.11.1999, C-151/98 P, Recital 25) in the context of the Regulation (EU) No. 2377/90. The CJEU found that the Court of First Instance

(ECJ) was right to hold that Article 8(3)(b) does not specify exactly the period within which the Commission must propose to the Council the measures to be adopted and that in using the expression "*without delay*" the Community legislature, whilst requiring it to act swiftly, did allow the Commission a certain degree of latitude.

87. Therefore, in accordance with the ruling of the CJEU the EDPB considers the term "*without delay*" in the context of Article 60(3)(1) as the obligation to act swiftly³⁰.
88. The fact that the legislator has inserted the term "*without delay*" in this context indicates that it has seen a need for action in terms of increasing the speed in the information flow connected with the draft decision. Nevertheless, due to the diversity of cases, no specific deadline could be determined in this respect. Therefore, the EDPB considers the term of "*without delay*" to mean that the information must be provided not literally immediately or in a specific timeframe but without hesitation, i.e. within a review period to be measured according to the circumstances of the individual case. In summary, that means that the LSA has to act proactively and, as quickly as possible, appropriately to the case. This of course applies as well to the reaction by the other CSAs to requests by the LSA.
89. To facilitate the planning of the other CSAs for their contribution to the draft decision, the LSA should consider how it is possible to support the scheduling of work of the other CSAs. This could be done for example, where appropriate, by the way of creating an indicative timetable.

Example 2: Prior to the investigation, the LSA proactively and quickly shares a timetable of the steps it intends to take. In due time, following the completion of the investigation, the LSA sends a summary of the results of the investigations to the CSAs in form of a note, with a short, reasonable deadline³¹ for comments in the context of an "informal consultation" in the EDPB Information system.

Following this, it shares the relevant information gathered and updates the timetable, adding a date for when it intends to share a preliminary draft decision, by when it requests comments by the CSAs on this preliminary draft decision and during which periods it intends to consult the affected parties.

90. As a best practice, the LSA and the CSAs may agree that the obligation to exchange relevant information "*without delay*" is fulfilled if there is a proactive, quick and comprehensive exchange of all relevant information, which enables the CSAs to screen, assess and react to it sufficiently early.

5.1.2 The term of "relevant information"

91. With regard to the concept of relevant information, reference can be made to the remarks provided under section 3.3.
92. Article 60(3)(1) establishes an information obligation of the LSA towards the CSAs in contrast to Article 60(1)(2), which regulates a mutual exchange of information between LSA and other CSAs. The communication of relevant information by the LSA according to Article 60(3)(1) in conjunction with

³⁰ In para. 115 of its opinion in the Case C 645/19 the Advocate General Bobek states that as a matter of principle, the GDPR requires, in cases concerning cross-border processing, the LSA to act promptly. Although acting promptly is not a synonym for acting swiftly, the EDPB considers that if the LSA acts proactively and as quickly as possible it also meets the requirements of acting promptly.

³¹ What is understood as reasonable has to be assessed on a case by case basis and may vary from a few weeks up to a month or more.

Article 60(1)(2) is ultimately related to the submission of the draft decision. Relevant information that is accessible only to the LSA should be transmitted to the other CSAs via the EDPB Information system.

93. The core idea of the cooperation procedure is that the consensus decision is reached and the case is resolved by collaborative interaction between the LSA and the other CSAs. Therefore, the other CSAs' involvement in the cooperation procedure is not limited to the right to express a relevant and reasoned objection pursuant to Article 60(4). In particular, before the creation of the draft decision the CSAs should be able to contribute to the overall procedure and may express their views also before the creation of the draft decision.
94. To that end, the LSA should in general endeavour to exchange preliminary results prior to submitting the draft decision, in particular, when divergent views could be expected, or when the other CSAs may need some time to familiarize themselves with the subject matter. This enables the LSA to be informed about the views of the other CSAs, in order to take these views duly into account already in preparation of the draft decision.

Example 3: At an early stage, after a preliminary examination of a complaint-based case, indicating further use of personal data for other purposes by business partners, the LSA shares this discovery with the other CSAs to seek an agreement on whether to proceed exclusively within the remit of the complaint or to extend the scope of the investigation into such secondary data processing.

Example 4: Upon conclusion of the fact-finding, the LSA provides a summary of the main results to the other CSAs, and, as appropriate in this case, also identifies key-issues for their consideration, in order to start building a common ground for the assessment of the merits of the case. This anticipated interaction between the LSA and the other CSAs proves essential to detect from the outset different points of view and, consequently, to promote as much as possible the necessary convergence.

Example 5: At a later stage, closer to the submission of the draft decision, all involved SAs have an overview of the facts and also an assessment of the potential infringements found during the investigation phase. These preliminary results and further evaluation include provisions that have possibly been violated and envisaged measures to be taken by the SAs under Article 58(2) and under Article 83(2).

95. As set out above and in the examples, the exchange of controversial or divergent legal views, as well as the exchange of views on complementary steps taken or not, and/or elements provided or not, should be general practice. This could prevent the discussion on different interpretations of the GDPR and the decision on them from being shifted to the dispute resolution procedure.
96. Nevertheless, where the LSA decides to trigger an inquiry on its own initiative and not on the basis of elements forwarded by the other CSAs, it does so within the remit of its discretionary power and, therefore, the views of the other CSAs cannot result in compelling the LSA to change the scope of its inquiry³².

³² Nonetheless, a CSA may raise, in a last resort situation, an objection regarding the scope as highlighted in para. 9 of the EDPB Guidelines 09/2020 on relevant and reasoned objection, provided that it meets all the requirements posed in Article 4(24), as explained in the Guidelines.

5.2 Article 60(3)(2): LSA's obligation to issue a "Draft Decision"

5.2.1 Legal obligation to submit a draft decision

97. Article 60(3)(2) sets forth an obligation on the LSA to submit a draft decision to the other CSA(s). This is shown by the use of the "*shall*" form coupled with the verb "*submit*", which entails a rule to be followed in all cases where Article 60 is applicable.
98. The submission of a draft decision under Article 60(3)(2) is an obligation applying to the LSA in the context of all OSS procedures. The competence of the LSA is grounded in Article 56(1), which is to be regarded as '*lex specialis*' whenever an issue arises in respect of cross-border processing operations. The competence of the LSA under Article 56(1) is exercised in such cases "*in accordance with the procedure in Article 60*"; therefore, the LSA acting within the framework of the OSS is bound by the provisions of Article 60, including Article 60(3)(2).
99. Accordingly, the LSA is required to submit a draft decision to the other CSAs in all cases, also when complaints are withdrawn by the complainant after the Article 60 procedure has been initiated or where no material (final) decision is issued according to national law.
100. Also in these cases, the draft decision serves as a final coordination between all supervisory authorities involved in the OSS procedure including the legal opportunities provided in Article 60(4) et seq. In complaint-based cases, the draft decision also provides the ground for the CSAs decisions pursuant to Article 60(8) and (9).

Example 6: After a complaint-based OSS proceeding has been initiated, the controller promptly eliminates the infringement after being approached by the LSA. In view of the case and the behaviour of the controller, the LSA concludes that the case may be closed. The LSA issues a draft decision stating its intention to close the case, which contains thorough reasoning for their course of action, and the remaining steps provided for by the Article 60 procedure are followed.

101. As explained in section 3.2 above and recalled by the EDPB in the RRO Guidelines 2/2020, "*the focus of all SAs involved should be on eliminating any deficiencies in the consensus-building process in such a way that a consensual draft decision is the result*". The LSA shall submit the draft decision to the other CSAs "*for their opinion*", i.e. the purpose is to consult the CSAs on the substance of the draft decision (see also reference in Article 60(4) to the "*consultation*" that the LSA is required to carry out "*in accordance with paragraph 3 of this Article*"). The consultation to which the submission of the draft decision is geared should therefore be seen in the light, once again, of the consensus objective underpinning the whole Article 60 mechanism (see the section 5.2.4 below on "*take due account of their views*").
102. As a best practice, the EDPB recommends that the LSA informs the other CSAs beforehand of the intention to submit a draft decision. This could be in line with an indicative timetable the LSA provided as part of the relevant information (according to Article 60(1)), in particular for cases which involve a large number of CSAs and/or which raise sensitive questions. In any case, knowing what is in the pipeline beforehand will help the CSAs organise their assessment of the draft decision and exploit the four-week deadline of Article 60(4) in full.
103. Regarding the "*submit*" part of the obligation, the EDPB recommends that such submission should only take place by way of the EDPB Information system so that certainty can be achieved as to the date of the submission, which is the starting point for the running of the four-week period mentioned in Article

60(4), and that all the CSAs can receive the draft decision simultaneously. This approach will ensure security and confidentiality of the submission and is also necessary in light of possible objections to the draft decision and disagreements between LSA and CSA, triggering the Article 65(1)(a) procedure³³. Use of the EDPB Information system appears to be the most appropriate channel to ensure a clear timestamp for the submission of the draft decision also in pursuance of Article 60(12).

104. As for the contents of the submission, in principle the draft decision should be such as to contain all the elements required for the CSAs to assess it (see section 6.2.2 below). Moreover, in particular for cases resulting in the adoption of a corrective measure and involving a large amount of relevant information exchanged to understand the reasoning and the analysis leading to the draft decision, the “relevant information” for the purposes of the draft decision should have been exchanged before submitting the draft decision in the light of the consensus objective underpinning the whole cooperation procedure. In other, simpler cases, where the draft decision is self-explanatory and no or very little relevant information needs to be exchanged, the relevant information may be shared along with the draft decision. Thus, in principle, the obligation under Article 60(3)(2) is for the LSA to submit only the draft decision as such.

105. Furthermore, the EDPB recalls that, where it is applicable under national law, the LSA should make sure that the draft decision it submits in this phase is fully compliant with the national law provisions regarding the right to be heard of the parties targeted by it (in particular the controller/processor at issue and the complainant, if a complaint has to be dismissed or rejected according to the applicable national laws). The LSA is therefore not required to submit, jointly with the draft decision and at the same time, such documents as may be necessary to provide evidence of compliance with the right to be heard, but it should reference the steps taken to ensure such compliance in the draft decision itself.

5.2.2 The term of “draft decision”

106. The submission of a draft decision is to be considered as one of the key elements within the cooperation mechanism as it constitutes on the one hand the decisive and final opportunity for mutual consultation on remaining disagreements and on the other hand, the only opportunity for the other CSAs to express reasoned and relevant objections.

107. The GDPR itself does not define the concept of the draft decision. In view of the meaning and purpose of the cooperation procedure, the notion of a draft decision at EU level should be subject to the development of common minimum standards to enable all involved SAs to participate adequately in the decision-making process.

108. According to Article 288(1) TFEU, a decision is an act of exercising [the Union’s] competences. In this context, the GDPR uses the terms of “tasks” (Article 57) and “powers” (Article 58) to establish the competences of data protection authorities.

109. Regarding legally binding measures supervisory authorities are empowered to take, a description of formal requirements can be found in Recital 129:

³³ Indeed, Article 11(2), letter d) of the RoP requires the LSA to provide “*documentation proving the timing and format of the provision of the (revised) draft decision*” to enable the Secretariat to verify that the draft decision (or revised draft decision) and the objections were submitted within the applicable deadlines.

- Written form
- Clear and unambiguous wording
- Indication of the SA which has issued the measure³⁴
- Date of issue of the measure
- Signature of authorised SA staff
- Reasons included
- Reference to the right of an effective remedy.

110. These formal aspects are in line with the ECJ case law on decisions of EU bodies as per Article 288(1)³⁵ TFEU as well as with the Charter of Fundamental Rights³⁶. Even though these provisions are supposed to regulate EU bodies, they provide guidance and may allow conclusions on the form and content of a draft decision as the respective competences are conferred on the SAs by Union law.

111. The previous conditions lead to the interpretation that every decision that is aimed at legal consequences needs to include a description of relevant facts, sound reasoning and a proper legal assessment. These requirements essentially serve the purpose of legal certainty and legal protection of the parties concerned. Applied to the area of data protection supervision this means that the controller, processor and complainant should be able to acknowledge all the reasons in order to decide whether they should bring the case to trial³⁷. Having regard to the decision making process within the cooperation mechanism, CSAs likewise need to be in the position to decide on possibly taking actions (e.g. agree to the decision, provide their views on the subject matter).

112. According to Article 60(3)(2) the term “*decision*” is modified by the prefix “*draft*”. A draft generally names a document, which is not final. It is an earlier version of the document that still needs a further step for completion. Apart from that final step, a draft contains all elements of the final document, but may be subject to further discussion or adjustment. As a result of such discussions, the draft can either be accepted by reviewers or modified according to their remarks. This is consistent with the wording of the GDPR, which states that the draft decision is to be submitted to the other CSAs “*for their opinion*”.

113. In order to fulfil their duties as CSAs in the framework of a cooperation procedure, it is necessary for the other CSAs to be able to assess the case on the basis of comprehensive documentation. The other CSAs need to be in the position to fully understand the case, the LSA’s conclusions and the reasoning, which have led to those conclusions.

Example 7: In order to be able to understand the appropriateness of a fine, the other CSAs must know the amount of the proposed fine and the specific circumstances of the assessment. This will regularly be explained in a comprehensible manner in the context of a decision that meets the above-mentioned minimum standards.

³⁴ This includes the dismissal/rejection of a complaint.

³⁵ Cf. ECJ, Joint Cases 11/66 (“*legal effects which are binding*”); ECJ, C 317/19 P (“*examine their complaint in sufficient detail and to give adequate reasons*”), ECJ, Joined Cases 8 to 11/66 (“*reasons for this decision with sufficient clarity*”); ECJ, C-24/62 (“*principal issues of law and of fact upon which it is based*”).

³⁶ Article 41(2)(c) CFR (“*obligation of the administration to give reasons for its decisions*”).

³⁷ See also: Recital 129, last sentence.

114. Taking into account the findings stated above, a draft decision is a provisional suggestion in the same form as a final decision would be. The only difference apart from procedural considerations between a draft decision and a final decision is that the step of the (final) consultation with the other CSAs has not been executed and the fact that the draft decision is not yet externally binding. If no relevant and reasoned objections according to Article 60(4) and (5) are expressed, the draft decision becomes legally binding for all SAs (cf. Article 60(6))³⁸.
115. In view of the aforementioned constitutional requirements for a legal decision within the meaning of Union law, and against the background of the meaning and purpose of the cooperation procedure, it appears necessary that the draft decision in the sense of Article 60(3)(2) corresponds in form and content to the decision that the competent SA is to adopt in the specific case. In this respect, the EDPB considers the notion "draft" to refer only to the provisional nature resulting from the mandatory involvement requirement of Article 60(3)(2).
116. In cases where complaints are withdrawn after the Article 60 procedure has been initiated or where no material (final) decision is issued according to national law, the draft decision should be modified as is appropriate to the case with a view to providing the findings in line with paragraph 113 above. This means that the draft decision must in any case indicate the intention of the LSA to close the case and sufficient reasoning appropriate to the case, which shall, at a minimum, enable the other CSAs to defend the case within their jurisdictions.
117. The EDPB points out further that, in principle, the existing information obligations under the cooperation procedure do not affect the form and content of the draft decision. Continuous transparency during all stages of the procedure is vital, but it does not affect the need for a proper description of the case and the legal assessment as a part of the draft decision itself.
118. The cooperation system designed by the legislator suggests that consensus on all relevant matters regarding the respective case should be strived for at an earlier stage by the competent SAs through continuous exchange of information. Therefore, the EDPB would like to emphasise that the focus of all SAs involved should be on eliminating any deficiencies in the consensus-building process in such a way that a consensual draft decision is the result.
119. These statements apply without prejudice to any additional requirements for decisions that may arise from respective national law.

5.2.3 The term of "without delay" regarding the submission of the draft decision

120. According to Article 60(3) (2), the LSA shall submit the draft decision to the other CSAs "*without delay*". A timely submission of the draft decision also alleviates the risks for the protection of the fundamental rights and freedoms of data subjects, since corrective measures taken in due time by SAs prevent continuing infringements.
121. As regards the legal characterisation of the term "*without delay*", the analysis carried out in section 5.1.1 above applies. Therefore, the LSA has to begin swiftly to create the draft decision in order to

³⁸ At this stage, it should be clarified whether the decision will be finalised via Article 60(7), (8) or 9. See para. 227.

submit it to the other CSA(s); nevertheless bearing in mind the complexity and the variety of cases, the timeline in which the LSA needs to submit swiftly the draft decision can be quite different.

122. What time is necessary for the submission of the draft decision must be assessed on the basis of an objective standard. The characteristics of the individual case and the overarching obligation to cooperate "*in an endeavour to reach consensus*" set out in Article 60(1), which in this case refers to the phase preceding the submission of the draft decision, shall be considered as well.

Example 8: A relatively straightforward investigation into a complaint regarding data subjects rights, whose outcome is to be disclosed to the other CSA as being relevant information pursuant to Article 60(3)(1), should enable the LSA to submit the draft decision shortly after the conclusion of the investigations.

In cases with complex findings and investigations, the LSA may be legitimised to take some time to submit the draft decision after the conclusion of the investigations (as made known to the CSAs)³⁹.

123. It should be pointed out that, pursuant to Article 41(1) CFR, the complainant has the right that his or her complaint is handled within a reasonable time. The ECJ has stated in a judgement of 8 May 2014 (C 604/12) that the right to good administration, enshrined in Article 41 of the Charter, reflects a general principle of EU law. This notion must also be respected in the execution of Union law throughout applying Member State administrative law like in the Article 60 procedure - all the more so considering that Recital 129 recalls that the powers of SAs (such as powers of investigation and corrective powers, including sanctions) should be exercised "*(...) fairly and within a reasonable time*". Thus, the timeframe with which a LSA may submit a draft decision in a complaint-based case should be such as not to entail that the handling of that complaint requires unreasonable time.

5.2.4 The term of "taking due account of their views"

124. To allow the LSA to take into account the views of other CSAs, the other CSAs are tasked with expressing their views as early as possible in the procedure. The views to be expressed are, thus, understood in a more extensive way than only relevant and reasoned objections. Indeed, Article 60(3)(2) refers to a broader concept than the mere consideration by the LSA of relevant and reasoned objections (Article 60(4) and (5)), including also comments, expression of support or remarks.

125. The EDPB considers that the LSA has the obligation to take due account of the other CSAs' views prior to and after the submission of the draft decision, as the obligation to endeavour to reach consensus pervades the entire cooperation procedure and is not terminated by the submission of the draft decision.

126. For this purpose, the draft decision should already address as much as possible the arguments and views shared by the other CSAs. Recital 125(2) states that the LSA should closely involve and coordinate

³⁹ It should be recalled that the need for a consensual scoping of the inquiries in the individual cases has been recognised by the EDPB in the RRO Guidelines 09/2020 (see para. 28): "*In procedures based on a complaint or on an infringement reported by a CSA, the scope of the procedure (i.e. those aspects of data processing which are potentially the subject of a violation) should be defined by the content of the complaint or of the report shared by the CSA: in other words, it should be defined by the aspects addressed by the complaint or report. In own-volition inquiries, the LSA and CSAs should seek consensus regarding the scope of the procedure (i.e. the aspects of data processing under scrutiny) prior to initiating the procedure formally.*"

the CSAs already in the decision-making process. To what extent this is necessary may vary from case to case.

127. The obligation for the LSA to take due account of the other CSAs' views in preparing the draft decision can also be inferred from the wording of Article 60(3)(2) to the extent that it relates to views expressed before the submission of the draft decision. The obligation for the LSA to take due account of the other CSAs' views after submitting the draft decision requires that the LSA considers not only relevant and reasoned objections but also comments or remarks, expressed during the period provided in Article 60(4) and (5).

128. The obligation to take due account means that the LSA will have to consider the views and arguments of the other CSAs in substance, using due diligence, as the cooperation procedure aims for a consensual decision.

129. As a best practice, the LSA should react to the views provided by all CSAs. The overarching obligation of endeavoring to reach consensus places concomitant obligations on both the LSA and the other CSAs. This means that the LSA is obliged to take account of all the views. However, the LSA is not obliged to follow each view that has been expressed. This is in particular the case where there are contradictory views among the other CSAs.

130. Article 60(3)(2) uses the wording "*take due account*" of the other CSAs views, whereas Recital 130(2) refers to "*take utmost account*"⁴⁰ of the view of the CSA with which the complaint has been lodged when taking measures intended to produce legal effects, including the imposition of administrative fines. The different wording ("*utmost*" instead of "*due*") reflects the specific role of the CSA with which the complaint has been lodged and suggests that this CSA's views have a more significant influence on the draft decision. This is due to the close link between this CSA and the case, because the CSA acts as a single point of contact for the complainant and, additionally, this CSA may be required to adopt and defend a decision, pursuant to Article 60(8) and (9).

6 ARTICLE 60(4) – ASSESSMENT OF THE OBJECTIONS AND POSSIBILITY TO TRIGGER A DISPUTE RESOLUTION PROCESS

6.1 Purpose of the provision

131. Article 60(4) concerns the period immediately following the submission of the draft decision by the LSA. Upon the submission, a four-week deadline begins to run during which any CSA may raise objections to the draft decision.

132. Within the individual provisions of Article 60, Article 60(4) has a unique position insofar as it establishes a link between the cooperation and consistency procedure. Where a CSA "*expresses a relevant and*

⁴⁰ In cooperation procedures under Article 56, in which the LSA has exercised its right under Article 56(4)(1) and decided to handle the case itself, the GDPR provides for an even more significant involvement of the CSA. In these cases, the CSA may submit to the LSA a draft for a decision according to Article 56(4)(2) and the LSA is expressly required to take "*utmost account*" of such draft. This wording suggests a higher threshold by introducing an even increased obligation for the LSA to consider the views of the CSA in comparison with "*take due account of their views*".

reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63." This deserves special attention in light of the fact that in this scenario the goal of reaching a consensus between the SAs, which is essential to the cooperation procedure, could not be achieved.

133. The EDPB recalls that the achievement of a consensual agreement on the outcome of the case is the ultimate goal of the whole procedure established by Article 60 and that reaching consensus should take priority over initiating the dispute resolution process. The duty of cooperation applies to every stage of the procedure and for all involved SAs. With regard to Article 60(4), this means that both other CSAs and LSAs should carefully follow the previous steps established in Article 60(1) and (3).

6.2 Relevant and reasoned objections by a CSA

134. After having been consulted by the LSA, in accordance with Article 60(3), the other CSAs may raise relevant and reasoned objections within a deadline of four weeks, since the CSAs must have been consulted "*in accordance with paragraph 3*".

6.2.1 Calculation of the deadline

135. The four-week period starts once the LSA has submitted the draft decision according to Article 60(3)(2) via the EDPB Information System. The calculation of the deadline for raising possible objections shall be done on the basis of Regulation 1182/71⁴¹. According to Article 3(2)(c) of Regulation 1182/71, "*a period expressed in weeks...shall start at the beginning of the first hour of the first day of the period, and shall end with the expiry of the last hour of whichever day in the last week...is the same day of the week, or falls on the same date, as the day from which the period runs*".

136. If an event from which a weekly period starts to run occurs, for example, on a Monday, the period also ends on Monday, in this case with the expiry of Monday (i.e. 11:59:59 p.m.) four weeks later.

137. The period includes public holidays, Sundays and Saturdays, since the GDPR does not expressly exclude these⁴². However, when the last day of a period is a public holiday, Sunday or Saturday, the period shall end with the expiry of the last hour of the following working day, thus the deadline ends on the following working day⁴³. Considering the European nature of the cooperation procedure, the holidays published in the official journal for the EU institutions⁴⁴ should be considered for the purpose of determining public holidays. Further, the time zone of where the EDPB is established should be used.

138. To avoid having the expiration date fall during the weekend, the initiator (i.e. LSA) should trigger the workflow only on working days and should make sure that the deadline does not expire on one of the EU holidays⁴⁵. In the spirit of cooperation, the EDPB encourages LSAs to consider the possible impact

⁴¹ Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits, Article 40 RoP confirms that "*In order to calculate the periods and time limits expressed in the GDPR and in these Rules of Procedure, Regulation 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits shall apply*".

⁴² Article 3(3) of Regulation 1182/71.

⁴³ Article 3(4) of Regulation 1182/71.

⁴⁴ Annually updated by Commission Decision, see for 2021: Commission Decision of 2 March 2020 on public holidays for 2021 2020/C 69/05 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020D0303%2801%29>); with the exception of the national holidays of Belgium and Luxembourg.

⁴⁵ As no automatic extension of the deadline is currently ensured in the EDPB Information system.

of extended holiday periods before submitting its draft decision to allow the other CSAs as much time as possible to react to its draft decision.

139. During the four-week period, a CSA may express one or more objections to the draft decision submitted by the LSA. However, in view of the requirements to raise relevant and reasoned objection(s) to the draft decision as a whole, the CSA should provide their objections in one single submission, though clearly distinguishing the different objections. This best practice will facilitate the analysis by the LSA and eventually by the EDPB, in case the dispute resolution mechanism is triggered. If, after inserting the objection(s) in the EDPB Information system, the CSA wishes to modify its submission, in any way and for any reason, this would still be possible, as long as this remains within the deadline provided for in Article 60(4). Therefore, the CSA should delete the previous version of the objection(s) and upload the new one in the EDPB Information system⁴⁶, so the submission available for the LSA and the other CSAs is always the updated text of the objection(s).

6.2.2 Relevant and reasoned objections

140. One of the key elements in this stage of the cooperation procedure is a common understanding of the notion of the term "*relevant and reasoned objection*". Article 4(24) defines relevant and reasoned objection as an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.

141. As the EU legislator suggested (end of Recital 124), the EDPB has issued guidelines on what constitutes a relevant and reasoned objection. The following paragraphs therefore only contain clarifications that are essential for the Article 60 procedure and are not already contained in the Guidelines 09/2020.

142. The right to raise an objection under Article 60(4) is available to each CSA individually and independently. Therefore, it does not depend on whether another CSA may already have raised an objection on the same matter. To the extent that a CSA objects on the basis of several items, each must separately meet the requirements for a relevant and reasoned objection under Article 4(24)⁴⁷. Consequentially, the mere endorsement of or referral to another CSA's relevant and reasoned objection does not constitute a relevant and reasoned objection on its own. In this context, for reasons of legal certainty as well as clarity and reliability within the objection process, the EDPB recommends that each CSA submit its own and complete (formal) objection to the LSA even if one CSA wishes to concur with the objection of another CSA⁴⁸.

⁴⁶ The EDPB Information system will automatically notify the LSA and other CSAs of the new addition.

⁴⁷ EDPB Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-092020-relevant-and-reasoned-objection-under_en.

⁴⁸ According to the EDPB Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679, referencing another objection cannot be seen as meeting the requirement of Article 4(24). In para. 7 the Guidelines clarify that "(...) a submission by a CSA should in principle explicitly mention each element of the definition in relation to each specific objection." Further, in para. 8 the Guidelines stipulate that "[t]herefore, the standard of "relevant and reasoned objection" is grounded on the assumption that the LSA's obligation to exchange all relevant information is complied with, allowing the CSA(s) to have an in-depth understanding of the case and therefore to submit a solid and well-reasoned objection."

143. In order to meet the threshold set by Article 4(24), a submission by a CSA should in principle explicitly mention each element of this legal definition in relation to each specific objection. If possible, as a good practice, the objection may also include a new wording proposal for the LSA to consider, which in the opinion of the CSA allows remedying the alleged shortcomings in the draft decision.

144. As required by Article 60(12), the CSAs shall submit the objections via an electronic and standardised format. The EDPB Information System shall be used for these purposes.

145. A mere “comment” expressed by a CSA in relation to a draft decision does not amount to an objection within the meaning of Article 4(24). The existence of comments shall therefore not give rise to the obligation to trigger the Article 65(1)(a) procedure if the LSA decides not to give any effect to the comment⁴⁹.

6.2.3 Assessment of the objections to the draft submitted under Article 60(4)

146. The LSA should make use of all possible means to exchange with the other CSAs on the issues raised in the relevant and reasoned objection. The EDPB recalls that the draft decision of the LSA should primarily be self-explanatory. Nevertheless, in response to an objection, the LSA should, also as a good practice, provide the CSA with explanation as to why a certain position has been taken in the draft decision, and it should as well provide the CSA with the opportunity to further explain its objections with undue delay. The LSA may also take the initiative to organise meetings, or otherwise use informal consultation to ensure that the reasoning employed by the respective authorities is understood.

147. After this further cooperation following the raising of an objection, the CSA may consider whether the LSA’s response adequately addresses its concerns and, if so, the CSA may consider withdrawing its objection⁵⁰. It may be the case in particular, when, following the LSA’s explanations, the conflicting views are only marginal in nature, in respect of the risks to the fundamental rights and freedoms of the data subjects.

148. If a CSA decides to withdraw its objection it should always explicitly identify the objection it intends to withdraw and be explicit that it wishes to withdraw said objection. This withdrawal may take place during the four-week period, or in case of a revised draft decision two-week period, following the submission of the draft decision, in which case the withdrawal should take place in the same EDPB Information system notification in which the objection has been raised. The withdrawal may as well take place after this period⁵¹. The LSA should make sure to document when this happened and notify this withdrawal to other CSA(s) without undue delay, via the EDPB Information system, as this information is to be understood as relevant information under Article 60(1).

149. When objections from different CSAs contradict each other on the assessment of a specific matter⁵², the LSA should indicate which objections it intends to follow and to what extend/how it intends to follow them. On the other hand, the other CSAs should carefully consider whether a withdrawal is

⁴⁹ See para. 17 of the EDPB Guidelines 03/2021 on Article 65(1)(a) GDPR (version for public consultation).

⁵⁰ After the period of the procedure expired, the CSA may consider not raising again its objection if the draft decision is to be revised.

⁵¹ As provided for in para. 27 of the EDPB Guidelines 03/2021 on Article 65(1)(a) a CSA may withdraw even after an Article 65(1)(a) procedure has been initiated..

⁵² A constant exchange of information between the SAs involved could prevent such situations.

appropriate in light of the opinions expressed by the LSA and/or other CSAs⁵³. It is important to remember that the overarching aim of Article 60 is for decisions to be made by consensus, insofar as possible. This goal regards the LSA as well as on the other CSAs.

6.3 Submission to Board

150. Article 60(4) provides for two alternative conditions, each of which has the effect of requiring the LSA to seek a decision from the Board:

- The LSA is of the opinion that the objection(s) is/are not relevant or reasoned.
- The LSA does not follow the relevant and reasoned objection(s).

151. In the first situation, the LSA is of the opinion that the objection submitted by the CSA does not meet all the requirements set out in Article 4(24), i.e. it considers that the objection is either not relevant and/or not reasoned, or both, in terms of whether there is an infringement of the GDPR and/or whether the envisaged action in relation to the controller or processor complies with the GDPR. In the second situation, the LSA considers the objection(s) to be both relevant and reasoned, but does not intend to follow them.

152. "*The matter*" to be submitted to the Board only concerns objections that the LSA does not intend to follow or that the LSA does not consider to meet the threshold stipulated in Article 4(24). Therefore, the items on which there is no dispute are not to be addressed via the dispute resolution under Article 65(1)(a).

153. Although Article 60(4) does not provide for an explicit time limit for the submission, the fact that a decision is pending which affects the risks to the fundamental rights and freedoms of the data subjects should result in the requirement of a submission as soon as possible as appropriate to the individual case⁵⁴.

154. On the other hand, in situations where the LSA wishes to follow some objections, but does not wish to follow other objections and/or does not consider them to be relevant and/or reasoned, the LSA should submit a revised draft in the procedure as per Article 60(5), according to the following section. The LSA should indicate clearly, through an informal exchange, which of the objections it intends to follow within the revised draft decision and how it intends to do so. Further, the LSA should indicate clearly, which objections have been noted as being the subject of a possible later dispute resolution via Article 65(1)(a)⁵⁵.

155. Nonetheless, as the revised draft decision is a new instrument, if they want to sustain their objections previously raised, the other CSAs will have to reiterate their position by (re)submitting their objections once the revised draft decision is shared. The EDPB is of the opinion that this course of action should be followed because it will allow relying on the dispute resolution procedure only for the objections that remain on the table in spite of the efforts made by all the parties to first seek a consensual solution.

⁵³ The CSAs should bear in mind that, should it come to a dispute resolution, the EDPB will adopt its decision based on a (qualified) majority vote.

⁵⁴ See also Recital 129, sentence 4 and 5.

⁵⁵ See also EDPB Guidelines 03/2021 on Article 65(1)(a).

7 ARTICLE 60(5) - THE REVISED DRAFT DECISION

7.1 Submission to the other CSAs

7.1.1 The LSA intends to follow

156. Article 60(5)(1) gives the LSA the possibility to follow a relevant and reasoned objection. It is important to note that to follow a relevant and reasoned objection means to follow such objection as it is, because the objection at issue is found by the LSA to be both relevant and reasoned and the LSA concurs with the reasoning.

157. The focus is on the “*intention*” to follow. The LSA’s intention to follow an objection is reflected in the fact that the LSA submits a revised draft decision. To what extent the revised draft decision does follow the relevant and reasoned objection as a whole raised by a CSA is, among other things, the subject of the procedure regulated by Article 60(5)(2) (see below, section 7.2), and ultimately by Article 65(1)(a) in case of disputes.

158. It should also be recalled that the threshold set forth by the EU legislator in the definition of a relevant and reasoned objection under Article 4(24) has to be met also in light of the manner the relevant and reasoned objection is to be structured by a CSA as set in the Guidelines 09/2020⁵⁶. This impacts the assessment of the relevant and reasoned objection by the LSA. Still, it is unquestionable that the intention to follow a relevant and reasoned objection is in line with the consensus objective underlying the whole Article 60 procedure. The revision should aim to completely address the risk posed by the initial draft decision as regards the fundamental rights and freedoms of the data subjects and, where applicable, the free flow of personal data within the Union that was identified in the objection.

159. The EDPB recalls that the LSA should make use of all possible means to exchange with the other CSAs on the issues raised in the relevant and reasoned objection. The LSA may take the initiative to organise meetings, or otherwise use informal consultation to ensure that the reasoning employed by the respective authorities is understood⁵⁷. In any case, this exchange should lead to the fact that the content of the revised draft decision does not come as a surprise to the other CSAs, as it should be the result of a sincere cooperation.

7.1.2 The obligation to submit a revised draft decision

160. The LSA is obliged to submit a revised draft decision if it intends to follow a relevant and reasoned objection, i.e. there is no alternative under the GDPR as clarified by the use of the “*shall*” auxiliary with the verb “*submit*”. Indeed, the alternative to submitting a revised draft decision can only consist in submitting the matter to the consistency mechanism as per Article 60(4) final sentence.

161. It should be pointed out that it is only a relevant and reasoned objection the LSA intends to follow that triggers the obligation on, and the possibility for the LSA to submit a revised draft decision under the GDPR. Article 60(5)(1) (and Article 60(4), for that matter) only refers to the “relevant and reasoned objection” submitted by a CSA – contrary to, in particular, Article 60(3), which refers to the “views” of the other CSAs⁵⁸.

⁵⁶ For details, see EDPB Guidelines 09/2020 on Relevant and Reasoned Objection para. 6-8.

⁵⁷ See also para. 146 et seq.

⁵⁸ See above in section 5.2.4 on “take due account”.

162. Accordingly, the fact that a CSA provided comments, remarks, observations to the LSA in the course of the four-week period mentioned in Article 60(4) which are not clearly and unambiguously declared as a relevant and reasoned objection does not entail an obligation or the possibility for the LSA to submit a revised draft decision. It should be recalled in this respect that both the LSA and the other CSAs are bound by the draft decision in case no objections are submitted “in the period referred to in paragraphs 4 and 5” pursuant to Article 60(6). This means that the LSA is m issuing a revised draft decision if no objections are submitted formally by the CSA, via the EDPB information system, in the four-week period set forth in Article 60(4) (more details in section 8)⁵⁹.

163. Should the LSA consider it necessary to nevertheless adapt its draft decision as submitted under Article 60(4) on account of factors or considerations supervening during the four-week period, including comments or remarks submitted by the other CSAs, or further submissions by the controller/processor, the LSA should withdraw its draft decision prior to the expiry of the four-week period and submit a new draft decision to the other CSAs. In doing so, the LSA should strike a balance between on one hand the importance of the factors or considerations supervening and on the other hand the need to ensure the expediency of the cooperation procedure⁶⁰. In all cases, the LSA should make clear to all the CSAs why it is withdrawing its draft decision by referring to the specific factor or consideration that is prompting it to take such a step. A new four-week period will start once the new draft decision is submitted. As said, this option is barred after the expiry of the above period in the absence of reasoned and relevant objections and the draft decision as initially issued becomes binding on the LSA and the other CSAs.

164. Considering the above, it is important for the LSA and the other CSAs to consult each other on how the LSA interprets the objections and how it intends to follow the objections.

165. Regarding the manner of submitting the revised draft decision, the same considerations apply as to the submission of the draft decision by the LSA⁶¹. A clear timestamp (date, hour) of the submission is the starting point for the two-week period referred to in Article 60(5)(2), therefore the revised draft decision shall only be submitted by way of the EDPB Information system.

7.1.3 The submission of the revised draft decision

166. As for the contents of the submission, the considerations made regarding the contents of the draft decision apply⁶². In short, the LSA is required to only submit a revised draft decision as such. The considerations made regarding the draft decision and the need to ensure compliance with the right to be heard⁶³ apply mutatis mutandis to the revised draft decision as well, so that the LSA should make sure that the revised draft decision references the steps taken to ensure such compliance and is self-explanatory regarding the changes introduced to follow the RRO and the underlying reasons⁶⁴.

⁵⁹ Comments signalling editorial errors and typos may however be taken into account to avoid material mistakes in the final decision.

⁶⁰ See the consideration regarding for instance the reasonable time for handling complaints mentioned in Recital 129.

⁶¹ See above in section 5.2.3 on Article 60(3)(2) on submission/timing.

⁶² See above section 5.2.2 specifying the term draft decision.

⁶³ See above para. 105.

⁶⁴ See also para. 159 as for informal exchanges prior to submission of a revised draft decision.

167. Article 60(5)(1) does not set any specific deadline for the submission of the revised draft decision by the LSA. This is one of the instances where there is a flexibility given to the SAs by the GDPR, also in order to facilitate the endeavour to reach a consensus. However, the principle of good administration, including the principles of reasonable timeframe and procedural economy still applies. Further, some factors that should be taken into account by the LSA in this respect include the following:

- the fact that a revised draft decision is subject to a shorter assessment period (2 weeks) compared to the draft decision;
- the reference to “*without delay*” applying to the submission of the draft decision under Article 60(3);
- the consideration made in Section 5.2.4 on Article 60(3)(2) as to the need to take account in this regard of the complexity of the case at hand, and here in particular of the number and nature of the relevant and reasoned objections received by the LSA;
- more generally, the obligation on all SAs to cooperate fairly and in a spirit of mutual trust.

168. All the above considerations would point to the need for the LSA to make sure that the lapse of time between receipt of the relevant and reasoned objections under Article 60(3) and submission of the revised draft decision is as short as possible and appropriate to the context of the OSS procedure. This is without prejudice to the efforts made to reach consensus and to the eventual obligation of the LSA to provide the right to be heard again, pursuant to national law, in view of envisaged changes in the revised draft decision that will newly affect the rights of the controller or processor.

7.1.4 The views of the other CSAs

169. The purpose of the submission of a revised draft decision by the LSA is to allow all involved SAs to find consensus and to gather their opinions on the proposed revised draft decision. It is important to note, in this regard, that the purpose of Article 60(5) is to afford the CSAs the opportunity to express a view on any amendments / revisions that have been made to the original text of the draft decision that was originally circulated by the LSA pursuant to Article 60(4). The wording “*for their opinion*” of Article 60(5)(1) mirrors, in this respect, the wording of Article 60(3)(2) (see above section 5.2.1).

170. This means that – like for the draft decision – the submission of a revised draft decision should be preceded by exchanges between the LSA and all the CSAs to share the new conclusions the LSA has reached in the light of the relevant and reasoned objection(s) it intends to follow along with the relevant reasoning, in order to gather the opinions of the other CSAs⁶⁵. This is especially appropriate if the relevant and reasoned objections address several issues in the case at hand, so that the extent and depth of the exchanges may vary from case to case. The LSA may for instance, where appropriate, share a preliminary revised draft decision before issuing the formal revised draft decision.

171. In turn, this will enable the other CSAs to flag remaining issues or questions that the LSA may wish to address at this stage, again in an endeavour to reach consensus, prior to the formal submission of a revised draft decision. In particular, the other CSAs should clearly indicate the points in respect of which they consider that the relevant and reasoned objections have not in fact been taken on board (i.e. followed) by the LSA. Ultimately, this informal consultation stage is intended to prevent the opinions by other CSAs from turning into relevant and reasoned objections to the revised draft decision

⁶⁵ At this moment, the LSA should as well take account of the views of the other CSAs raised as comments.

and therefore from triggering the next steps in the procedure as outlined in the following section, with all the relevant consequences.

7.2 The Revised Draft Decision: Assessment Procedure

7.2.1 Joint application of Article 60(5) second sentence and the procedure of Article 60(4)

172. Article 60(5)(2) sets forth the formal procedure applying to the examination of the revised draft decision by the other CSAs. This procedure is the one referred to in Article 60(4), with the difference that the timeline is limited to two weeks⁶⁶.
173. It should be noted that, by referencing Article 60(4), (5)(2) also regulates the procedure to be followed by the LSA in case it rejects or does not follow any relevant and reasoned objection to the revised draft decision as expressed by other CSAs in the two weeks following submission. This has several consequences:
174. In both cases the only outcome envisaged according to the procedure provided for under Article 60(4) is the submission of the matter by the LSA to the consistency mechanism, i.e. to the EDPB (as described in Section 6.2.3) with a view to a binding decision settling the dispute, which the LSA and other CSAs are then required to abide by (under Article 65(2) and (6)).
175. If no objections are raised by the other CSAs in the two-week period mentioned in Article 60(5)(2), Article 60(6) applies. Subsequently, the revised draft decision becomes binding on both the LSA and other CSAs, since Article 60(6) refers to the absent submission of relevant and reasoned objections within the periods referred to “*in paragraphs 4 and 5*”.
176. Thus, if relevant and reasoned objections are raised in the two-week period and the LSA intends to follow them, the only alternative is to apply Article 60(5)(1) again, in order to ultimately achieve the agreement on the (revised) draft decision, as per Article 60(6), which will become then binding for both the LSA and other CSAs.
177. This would be in line, on the one hand, with the endeavour to reach consensus, as prescribed by Article 60(1), and on the other hand, it would prevent triggering Article 65(1)(a) when there is no dispute to be settled at this point. Indeed, Recital 138 clearly supports such an approach, in that all means within the cooperation mechanism should be exhausted before activating the consistency mechanism.
178. Nevertheless, considering the enhanced cooperation procedures as outlined in this guidance (e.g. exchange of relevant information in different stages and informal consultation before submitting a draft decision), this situation should be very exceptional and limited to the cases where, despite all efforts, specific circumstances did not allow reaching a consensual position before.
179. However, it shall be borne in mind by the other CSAs and the LSA that the GDPR provides for a swift action and for the powers of the SAs to be exercised fairly and within a reasonable time, as mentioned in Recital 129. Actually, it can be argued that it was not the intention of the legislator to promote an indefinite loop of revised draft decisions. For that reason, the possible submission of new revised draft decisions should be of an extraordinary character, as necessary in the particular case to strive for final consensus.

⁶⁶ See above section 6.2.1 for Calculation of the deadline.

180. Recognising that the endeavour to reach consensus set forth as an overarching objective of the cooperation procedure in Article 60(1) does not entail an obligation to achieve consensus at all costs, when the LSA mindfully intends to follow a relevant and reasoned objection, and, by this way, achieve such goal, that should be made possible by submitting a (re-)revised draft decision.

181. Where the LSA concludes that consensus is not possible, as there is no substantive convergence between the LSA and other CSA(s), either because there are contradictory views from CSAs or because some legal issues remain unsettled, the LSA is then obliged by Article 60(5)(2) to prompt the procedure provided for in Article 60(4) and, consequently, to refer the case to the EDPB for the dispute resolution procedure as per Article 65(1)(a).

7.2.2 Constraints on other CSAs in submitting relevant and reasoned objections to the revised draft decision

182. A further issue to be considered concerns the scope of the “*procedure referred to in paragraph 4*” as applied in the context of Article 60(5)(2). This refers in particular to whether specific legal constraints apply on either the CSAs or the scope of a relevant and reasoned objection to the revised draft decision issued by the LSA.

183. It should be recalled that the LSA and other CSAs are bound by the (revised) draft decision under Article 60(6) only if no objections have been submitted to the (revised) draft decision. If this is not the case, i.e. if relevant and reasoned objections were indeed raised to the draft decision pursuant to procedure provided for under Article 60(4), then no CSA is bound by the draft decision; moreover, the revised draft decision submitted by the LSA under Article 60(5)(1) is a different legal instrument compared to the draft decision mentioned in Article 60(4). Accordingly, a CSA may raise a relevant and reasoned objection to the revised draft decision even if it had not raised any objections to the draft decision during the four-week period mentioned in Article 60(4).

184. Indeed, the changes introduced by the LSA to follow the relevant and reasoned objections may raise new questions and issues a CSA disagrees with in the context of the revised draft decision. As per the above guidance, the CSA should make sure that each relevant and reasoned objection it submits should “*indicate each part of the draft decision [here: revised draft decision] that is considered deficient, erroneous or lacking some necessary elements, either by referring to specific articles/paragraphs or by other clear indications*”⁶⁷.

185. The EDPB strongly encourages the LSA to share in advance its intention to revise the draft decision not only to the CSA that has raised an objection but also to all other CSAs. This will ensure that the revised draft decision and the reasoning employed will not come as a surprise to the other CSAs, and will help in preventing their possible negative reaction on the proposed changes.

186. The aim of a revised draft decision within the meaning of Article 60(5) is to endeavour to find consensus on issues for which no consensus was previously found. As a result, a CSA should not raise a relevant and reasoned objection in relation to a revised draft decision if there was previously no relevant and reasoned objection directed at that specific issue and the LSA has not revised the draft decision in respect of such issue.

⁶⁷ See EDPB Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 para. 7.

8 THE BINDING EFFECT OF A (REVISED) DRAFT DECISION

187. Article 60(6) describes the final step of the decision finding process in cases in which a consensus between the LSA and other CSAs could be reached. In this case, consensus is signalled by the absence of objections to the (revised) draft decision, which means that Article 60(6) is applicable. This has two legal consequences:

- that the LSA and other CSA(s) are deemed to be in agreement,
- that they are bound by the decision in the sense that the assessment process following the issuing of the draft decision came to an end.

8.1 Deemed to be in agreement with the draft decision

188. Firstly, Article 60(6) states that, in the absence of an objection, the SAs shall be deemed to be in agreement with the (revised) draft decision in its entirety. The term "*deemed to be in agreement*" clarifies that the CSAs do not have to explicitly endorse the (revised) draft decision. The GDPR provides for a tacit agreement and supposes that the SAs have successfully reached consensus in the cooperation procedure. This tacit agreement refers to the content of the (revised) draft decision.

8.2 Bound by the draft decision

189. Since the LSA and other CSAs are presumed to be in agreement, they shall be bound by the content of the (revised) draft decision. This has immediate binding effects for all involved SAs. This means, that any further adoption of a measure under national law, such as the dismissal of a complaint, has to be strictly in line with the agreed draft decision.

190. Two different dimensions of the binding effect can be distinguished, i.e. as regards the entities bound by the (revised) draft decision (LSA/CSAs) and the scope of that (revised) draft decision.

191. Firstly, both the LSA and other CSAs are bound by the (revised) draft decision because no objections were raised or maintained. The legal consequences of the binding effect are that in this case the (revised) draft decision cannot be changed further or withdrawn afterwards⁶⁸. The decision to be adopted by the LSA (Article 60(7)) or by a CSA (Article 60(8)) or in a shared form by both SAs (Article 60(9)) shall be based on the (revised) draft decision as it is.

192. The decision only binds the LSA and the other CSAs that participated in the cooperation procedure. Only SAs which have participated in the cooperation procedure (i.e. which have formally confirmed their role as a CSA in the context of this Article 60 procedure), and had the opportunity to raise a relevant and reasoned objection against the draft decision can be bound by a decision which was taken in that procedure. The other SAs neither had the opportunity to present their views in the cooperation procedure nor could raise a relevant and reasoned objection against the draft decision.

193. Therefore, if a CSA with a complaint which could be handled within the ongoing procedure asks the LSA to include its case in this procedure and join the cooperation procedure prior to the submission of the draft decision and had the opportunity to raise a relevant and reasoned objection, the procedure

⁶⁸ In certain exceptional cases provided for by law such changes or withdrawal might still be necessary; see para. 207.

can continue and the “new” CSA will be bound by the draft decision provided that the requirements of Article 60(6) are met.

194. Conversely, if a CSA with a complaint which could be handled in the ongoing cooperation procedure only sends its case to the LSA to be bundled with the other(s) after the deadline of Article 60(4) or Article 60(5) has expired (e.g. because a SA received a complaint referring to the same infringement after the expiry of the deadlines), and, therefore, had not had the opportunity to express a relevant and reasoned objection, this CSA should very carefully consider whether a new cooperation procedure should rather be triggered for that purpose, as by requesting the LSA to bundle the new case within the ongoing procedure at this stage, this CSA is de facto waiving its possibility to raise an objection to the decision⁶⁹.

195. The EDPB considers that, in principle, the LSA is not required to continuously check that all possible relevant CSAs with cases, which could be bundled to the ongoing procedures being dealt with, are informed about the ongoing cooperation procedure.

196. The binding effect granted by Article 60(6) to the specific decision is thus strictly limited to the specific cooperation procedure. The cooperation procedure deals with a specific issue and aims to reach consensus regarding the specific case.

197. Therefore, besides the binding effect of the decision as per Article 60(6), the outcome of a given cooperation procedure may not be automatically extended to other cooperation procedures, in spite of possible similarities. However, according to Article 51(2), each SA shall contribute to the consistent application of the GDPR and therefore, the LSA may reuse the text and conclusions of a draft decision agreed upon in a previous cooperation procedure involving the same or different controller and the same infringement of the GDPR to speed up the procedure at hand if it considers that this can facilitate reaching an agreement also in the current case.

198. The EDPB considers that the binding effect under Article 60(6) of a specific decision cannot cover the clarification of abstract legal questions, which are not connected to the real case. A SA that intends to ask the EDPB for clarification of abstract legal questions should instead consider the Article 64(2) procedure if the question refers to a matter of general application or producing effects in more than one MS.

9 ARTICLE 60(7) – THE LSA ADOPTING AND NOTIFYING THE DECISION

9.1 General

199. Article 60(7-9) address the different scenarios after the LSA and other CSAs have been bound by the draft decision. These steps can be reached after:

- (i) either the procedure laid down in the previous chapter has been concluded and consensus has been reached, or
- (ii) after a dispute resolution by the Board has been concluded.

⁶⁹ See above para. 22 et seq.

200. The abovementioned paragraphs outline:

- (i) which SA shall adopt a final decision following the previous steps, and
- (ii) which SA notifies or informs the controller, processor and complainant respectively.

201. Article 60(7) provides the procedure to follow in case a decision targeted at the controller or processor is to be adopted by the LSA. Article 60(8) and (9) are only relevant in complaint-based cases. Article 60(8) regulates the cases where the decision dismisses or rejects the complaint and should be adopted by the complaint receiving SA(s)⁷⁰. Finally, Article 60(9) clarifies the procedure to be followed where some parts of a complaint have been dismissed or rejected, and the respective decision is adopted towards the complainant by the complaint receiving SA, while other parts have been acted upon, leading to a decision towards a controller or processor by the LSA.

202. Due to this relation, many of the concepts and considerations related to Article 60(7) will be analogously applicable for Article 60(8) and (9).

9.2 Adoption of the final decision by the LSA

203. Article 60(7)(1) stipulates that the LSA will be required to adopt a decision. This adoption is either:

- the implementation by way of a national decision of the consensus reached under Article 60(6), and/or
- the implementation by way of a national decision on the basis of the binding decision of the EDPB adopted under Article 65, following the procedure provided under Article 65(6).

204. In either case, the national decision needs to give full effect to the binding consensus reached under Article 60(6), and/or to the binding directions set out in the EDPB's decision under Article 65⁷¹.

205. At the same time, the LSA will need to adjust the format to comply with its national administrative rules. Lastly, it will be able to make purely editorial changes before adopting its national decision⁷².

206. Article 60(7) does not stipulate a concrete timeframe within which this adoption has to take place. Nonetheless, the adoption should take place as swiftly as possible, in line with the principle of good administration. In contrast, if this point was reached following a consistency procedure, the deadline of one month provided by Article 65(6) has to be followed.

207. However, there could be exceptional situations, where adopting a decision, which is implementing the conclusions to which the SAs are bound under Article 60(6) would affect the legality of the national decision. This may be due to a ruling by the CJEU with an interpretation different to which the other CSAs and the LSA are bound or a change in legislation. In case of such circumstances, the CSA who becomes aware of those new facts should immediately inform the LSA and vice versa. Following this, the LSA should inform the other CSAs accordingly and submit to the other CSAs a new draft decision

⁷⁰ Article 60 gives the CSA(s) that have received a complaint, which is subject to the procedure, a special role. This is further elaborated in the part on Article 60(8) and Article 60(9). To avoid confusion between these SAs and other CSAs, the term *complaint receiving SA* is used. It is important to note that even the LSA can have the role of a complaint receiving SA.

⁷¹ See para. 114 and para. 192. See also para. 50 of EDPB Guidelines 03/2021 on the application of Article 65(1)(a) GDPR - version for public consultation.

⁷² See footnote 58.

that takes account of the changed circumstances. This new draft decision should be aligned as much as possible with the previous draft decision, to make use of the already found consensus.

9.3 Notification and information

208. Once the decision has been adopted, the LSA shall notify the decision to its addressee(s). In complaint-based cases, the complaint receiving SA(s) shall also inform the complainant(s) of the decision. While the terms “*notify*” and “*inform*” are not specified in the GDPR, they may be specified in national law. However, the CJEU clarified that the duty to notify is satisfied when the addressee is placed in a position in which it can effectively become aware of the existence of the decision and the reasons why the institution intends to justify it⁷³.
209. In line with the above, Article 60(7-9) appears to give the term “*notify*” a more formal value, as it is used for the communication to the party that may suffer adverse effects by the decision, and therefore may intend to challenge it⁷⁴.
210. Therefore, for Article 60(7-9), when notifying the decision to the addressee, the SA should provide a full copy of the decision in a language complying with its national laws. Additionally, the MS in which the decision was notified will be the MS in which the decision may be challenged and, as outlined below, it should be brought to the attention of the parties that were merely informed that judicial action should be sought in such MS.
211. In any case, in the context of Article 60(7), after the LSA has notified the decision⁷⁵ to the main or single establishment of the controller or processor, as the case may be, it shall inform the other CSAs and the Board of the decision in question, including the information specified in the subsection below. For this purpose, the SA should make use of the Article 60 Final Decision notification procedure in the EDPB information system.
212. Besides ensuring transparency towards the CSAs, providing this information to the Board is essential to allow the SAs to comply with their obligation to contribute to the consistent application of the GDPR as stipulated in Article 51(2). This will allow them to avoid an inconsistent application of the GDPR should they in the future need to handle a similar case.
213. The complaint receiving SA(s) is then required to inform the complainant of the outcome of the complaint, in accordance with its national laws and/or practices. Additionally, the complaint receiving SA(s) should inform their complainant(s) pursuant to Article 77(2) that they may seek judicial remedy before a court in the MS of the LSA, if they are concerned by the decision of the LSA in the meaning of Article 78(1)⁷⁶.

Example 9: After a media report casting doubt about the lawfulness of the processing conducted by HappyCompany, multiple individuals file a complaint with their local SA. Once the LSA has been identified, it decides to handle the complaints, as they refer to the same processing activity and the same infringement, in one file. Following the adoption of a decision by the LSA and the notification of

⁷³ See for more C-6/72 Section 15 p.2, joint cases T-121/96 and T-151/96, p. 40, joint cases C-115, 116/81 p. 13

⁷⁴ See also para. 55 of EDPB Guidelines 03/2021 on the application of Article 65(1)(a) GDPR, Article 78 and Recital (143) GDPR.

⁷⁵ See also section 5.2.2 on the term of “*draft decision*” for formal requirements.

⁷⁶ The complaint receiving SA should be able to identify the relevant court based on the adopted decision shared by the LSA.

the controller, each of the complaint receiving SAs informs their respective complainants on the decision. When doing so, the complaint receiving SAs also inform their complainants that they can effectively seek judicial remedy in the MS of the LSA.

214. At this moment, the LSA should as well inform the controller or processor of its obligations under Article 60(10) and the possible consequences of non-compliance.

9.4 A summary of the relevant facts and grounds

215. When the LSA informs the other CSA(s) and the Board, it provides a summary⁷⁷ of the relevant facts and grounds regarding the decision in question. This summary should include the formal steps and grounds, as well as the substance, of the decision.

216. Therefore, the summary should include, at least, the following information⁷⁸:

- The date of the final decision;
- The identification of the LSA and other CSAs;
- The name of the controller(s) and/or processor(s);
- The relevant legal conclusions in question (infringed provisions/rights not granted⁷⁹), in relation to the factual basis of the case⁸⁰;
- The outcome of the procedure and, if applicable, the corrective measures taken⁸¹.

217. As the case may be, the summary should allow any Member of the Board to understand the subject matter and conclusion of the decision reached. It is recommended that the LSA also provide a copy of the decision in English. This should be done by making use of the appropriate fields in the EDPB information system.

10 ARTICLE 60(8) –THE DISMISSAL/REJECTION OF A COMPLAINT

218. Article 60(8) concerns the situation where the CSAs including the LSA have agreed to dismiss or reject a complaint in full, or where this was concluded by the EDPB following Article 65. The SA with which the complaint was lodged can be either the LSA or another CSA. It introduces three obligations on the SA with which the complaint was lodged:

- to adopt the decision,
- to notify it to the complainant,
- to inform the controller.

This is to be done by derogation from Article 60(7).

⁷⁷ This is separate from a summary of the decision.

⁷⁸ This information is contained in the fields that are to be filled out in the “final decision” form in the EDPB Information system.

⁷⁹ This could be due to restrictions under Article 23.

⁸⁰ See for instance the fields “Description of the Cooperation Case” and “GDPR Legal reference”.

⁸¹ See for instance “Kind of Decision”.

10.1 Derogation from paragraph 7

219. Article 60(8) introduces a derogation from the situation where the LSA adopts and notifies the decision to the main, or single, establishment of the controller or processor in the EU. It applies solely in the situation where a complaint is dismissed or rejected in full.

220. Although in general, in the OSS mechanism, the LSA should remain the sole interlocutor of the controller/processor for their cross-border processing, in this specific situation a CSA has to inform the controller/processor about the dismissal or rejection of the case.

10.2 The term “Dismissal/Rejection”

221. The concepts of dismissal and rejection may have different definitions at national level, and therefore also different procedural/administrative implications. However, the GDPR does always refer to both actions, a dismissal or a rejection⁸².

222. The CJEU has consistently held that the terms of a provision of EU law which makes no express reference to the law of the MS for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the EU, having regard not only to its wording but also to the context of the provision and the objective pursued by the legislation in question. This follows from the need for uniform application of EU law and from the principle of equality⁸³.

223. Regarding more specifically the interpretation to be given of what dismissal/rejection entails, reference can be made to the wording of Article 60(9) where dismissal/rejection are contrasted with a decision to “act on” the complaint. It should be noted that Article 60(9) refers to the LSA adopting the decision “*for the part concerning actions in relation to the controller*”, in which case the decision will be notified by the LSA to the controller/processor, whilst it refers to the CSA adopting the decision “*for the part concerning dismissal or rejection of that complaint*”, in which case the decision will be notified by the complaint-receiving SA to the complainant. Thus, Article 60(9) read jointly with Article 60(8) can be interpreted in the sense that dismissal/rejection of a complaint as the outcome of an Article 60 procedure entails that the (part of the) final decision to be adopted does not contain any action to be taken in relation to the controller.

224. From this standpoint, such a decision can be considered to adversely affect the complainant. This is confirmed by the GDPR legislative process, where a more general reference to decisions “*adverse*” to complainant was made⁸⁴. The explicit reference to the right to judicial remedy and proximity to the complainant (as recalled above in particular in paragraph 213) also suggests that adverse decisions for the complainants should fall within this category. When the complaint is not followed at any level in the final decision and the LSA does not take any action in relation to the controller/processor in that

⁸² The CSAs will have agreed beforehand on the substantive consequences of the decision. The implementation of the consequences has to be done in line with national law, e.g. via a rejection or via a dismissal.

⁸³ See e.g. Case C-617/15, Hummel Holding, para. 22 and case law cited therein.

⁸⁴ See <https://data.consilium.europa.eu/doc/document/ST-14788-2014-REV-1/en/pdf>. In this version, the provision read: “*Where the decision jointly agreed upon concerns a complaint and as far as it adversely affects the complainant, notably where the complaint is rejected, dismissed or granted only in part, each supervisory authority that have received such complaint shall adopt the single decision concerning that complaint and serve it on the complainant.*” p. 36.

decision, the controller/processor will not have an interest in a judicial remedy within the MS of its main establishment. The complainant on the other hand, will have an interest in challenging the decisions adversely affecting him/her within their own MS, and in their own language⁸⁵.

225. Thus, a decision dismissing or rejecting a complaint (or parts of it) should be construed as a situation where the LSA has found, in handling the complaint, that there is no cause of action regarding the complainant's claim, and no action is taken in relation to the controller. In such case, the complaint has to be dismissed or rejected via the decision adopted by the complaint receiving SA, as the case may be⁸⁶.

226. Notification received in application of Article 60(8) can be used by the complainant to exercise the right to judicial remedy against the decision taken by a SA. Because this decision has to be adopted by the complaint receiving SA, this will allow proximity of the complainant to the competent court, under Article 78(3) and under Article 47 of the Fundamental Rights Charter (by seizing a court in the complainant's MS as the decision will be adopted by the CSA in that MS)⁸⁷.

227. This means that, for the purpose of the application of Article 60(8) and (9), and of the final sentence of Article 60(7), the decision that is the outcome of the cooperation procedure should clearly provide for the dismissal or rejection of the complaint, or for the action to be taken in relation to the controller by the LSA, so that the LSA and CSA can direct the subsequent adoption of the respective national decisions accordingly, in pursuance of Article 60(8), (9) or (7).

228. If provided in national law, SAs should rely on these definitions of dismissal/rejection, as well as in the national administrative practices that configure a case of dismissal/rejection of a complaint, and proceed, in such cases accordingly⁸⁸. In any case, the draft decision, shared as indicated in the previous sections, should provide clear reasoning as to why the complaint is dismissed/rejected under the relevant national laws.

229. It is important to note that a dismissal or rejection at this stage is different from a possible finding of dismissal or rejection at the vetting stage of the complaint procedure. As highlighted in paragraph 50, this vetting precedes any submission of the complaint to the LSA and is performed by the complaint receiving SA. In such a case, the complaint would be dismissed or rejected before reaching the cooperation stage.

230. It should also be acknowledged that there may be situations where the interests of the data subject are not adversely affected by the outcome of the OSS procedure, on account of the steps taken by the LSA in the course of handling the complaint. In such cases, the key factor is the demonstrated removal

⁸⁵ See also the A.G. Opinion in case C-645/19 Facebook. In para. 105 the Opinion states:

"These mechanisms of shifting the competence to adopt the decisions and, where necessary, of potentially adopting two-tier decisions (the LSA vis-à-vis the controller or processor, and the local authority vis-à-vis the complainant) seem specifically intended to avoid data subjects having to 'tour' the courtrooms of the European Union in order to bring proceedings against inactive supervisory authorities."

⁸⁶ Possibly in conformity with the applicable national provisions where they do define the precise scope of dismissal/rejection.

⁸⁷ See Recital 141: "*the right to an effective judicial remedy in accordance with Article 47 of the Charter (...)* where the supervisory authority partially or wholly rejects or dismisses a complaint (...)".

⁸⁸ The SAs should make sure that the application of such definitions is consistent with the understanding of the terms as set out in this section.

of the cause of action - that is to say the complainant obtained the vindication of his/her rights through the intervention of the LSA towards the controller, which meanwhile met the terms of the complainant's claim. In such cases, providing that the complainant has been informed in the course of the procedure about the favourable result achieved, the LSA may decide to no longer take action in relation to the controller – i.e. none of the factors mentioned above in respect of dismissal/rejection vs. taking action is applicable.

231. This is the case, in particular, with the amicable settlement situation - i.e. the situation where the case has been resolved to a satisfaction of a data subject, when the infringement alleged in the complaint has been identified by the LSA and when the complainant agreed to an amicable resolution of this complaint. This situation falls within the remit of Article 60(7). Indeed, as already pointed out, the decision does not adversely affect the complainant, who manifested his or her satisfaction with the proposed settlement, and as such is not to be adopted by the complaint receiving SA under Article 60(8) or (9) – there being no dismissal or rejection at play. It will be for the LSA to adopt the final decision in such a case⁸⁹, to take stock of the achieved settlement in its capacity as the sole interlocutor of the controller/processor under Article 56(6).
232. This also applies to cases that do not fall within the amicable settlement constellation, as the LSA did not or could not attempt such a settlement, but, nevertheless, its intervention during the handling of the complaint led the controller to stop the infringement and fully satisfy the complainant's claim. In view of this result and of the specific circumstances of the case, the LSA may consider that the most adequate decision for the complaint at hand is to terminate the handling of the case, taking note of the achieved solution, and without taking any action towards the controller⁹⁰.
233. However, since an infringement was indeed identified by the LSA, the decision not to take any action towards the controller would have to be based on the careful assessment of the circumstances of the complaint as a whole, in order to keep the same level of guarantees afforded to the data subjects.
234. On the other hand, within this context the final decision will not be issued by the complaint receiving SA but instead by the LSA, as per paragraph (7), even though no action is to be taken in relation to the controller through such final decision – in recognition of the LSA's role as the sole interlocutor of the controller targeted by the complaint at issue and the fact that a finding of an infringement can have an adverse effect on the controller. This would render it impossible for the complainant to challenge the decision in the MS where the complaint was lodged, regardless of whether the complainant still has or has not cause of action to seek judicial remedy against a SA. That is a matter for the courts to determine in the concrete case. Therefore, whenever this scenario may happen, it should be ensured by the LSA via the complaint receiving SA that the complainant is duly informed on the positive achievement and on the envisaged outcome of the complaint and expresses no disagreement.
235. Lastly, it should be recalled that also the decision not to take action towards the controller, even when an infringement took place, has to have been agreed by the LSA and other CSAs, which entails that all

⁸⁹ As this is the general rule, see also ECJ Case C-645/19 para. 56 : "In accordance with Article 60(7) of that regulation, it is the responsibility of the lead supervisory authority, as a general rule, to adopt a decision with respect to the cross-border processing concerned..."

⁹⁰ This is without prejudice to the assessment on what is "the extent appropriate" to which the complaint is to be investigated pursuant to Article 57(1)(f), for which discretion lies with the SAs.

the circumstances of the case were duly taken into account, including the guarantee of the rights and freedoms of the complainant.

Example 10: Unhappy customer submits a complaint to its local SA in MS A. The SA performs the preliminary vetting and forwards the complaint to the LSA. After receiving the complaint, and, upon investigating the issue, the LSA cannot find evidence to support the complaint. Therefore, the LSA is unable to determine the infringement and concludes that the complaint is to be rejected/dismissed, as no action is taken on the controller. The LSA shares a draft decision to that effect and as no objection is raised, pursuant to Article 60(8) the complaint receiving SA will adopt the final national decision rejecting/dismissing the complaint and notify it to the complainant.

Example 11: A complainant indicates he sent a request to a controller and did not receive any answer. The DPA does not receive any response to its preliminary vetting actions. The complaint receiving SA sends the case to the LSA. The LSA notes that the request was sent to a wrong/non-existent address by comparison to what is indicated on the website of the controller (the complainant seems to have tried a contact@XXX.com address without checking the contact addresses mentioned on the website). The LSA shares a draft decision whereby the complaint is to be dismissed/rejected since there was only a mistake made by the complainant. As no objection is raised, the complaint receiving SA adopts the final dismissal/rejection decision under Article 60(8) and notifies it to the complainant.

Example 12: Unhappy customer submits a complaint to its local SA in MS A, arguing that the website HappyCompany is infringing its rights. After performing the preliminary vetting the complaint is transferred to the LSA in MS B. The LSA starts an investigation but cannot access the website in question. After some further research, it finds that in the meantime the controller has been dissolved. Therefore, the investigation cannot be continued and the LSA cannot find sufficient evidence to support the claims of the complainant. The LSA shares a draft decision that the complaint should be dismissed as the cause of the complaint has disappeared. As no objection is raised, the complaint receiving SA adopts the final national decision dismissing/rejecting the complaint under Article 60(8), and notifies it to the complainant.

Example 13: Unhappy customer submits a complaint to its local SA, arguing that her data are kept and processed unlawfully by HappyCompany, which is infringing her rights. After performing the preliminary vetting the complaint is transferred to the LSA. The LSA starts an investigation and is informed by controller that indeed the complainant's data are kept in their files on account of a failure in their customer resource management that did not erase the information in due time (preferences, purchase history, etc.); however, they immediately erased the information following the letter sent by the LSA, and proof of this is provided to the LSA. Therefore, the LSA shares a draft decision where it finds an infringement by the controller and it represents the situation as remedied following the LSA's intervention, without proposing any corrective measures in respect of the controller in particular because this was the first time such an infringement was committed. Accordingly, the LSA proposes to go for the option of adopting the final decision itself under Article 60(7). As no objection is raised, the LSA adopts a final national decision along the said lines and notifies it to the controller, whilst the complaint-receiving SA will inform the complainant of such decision.

10.3 Adoption of the decision

236. The SA that is required to adopt the decision is the SA, which received the complaint(s). This could apply to multiple SAs. It should do so in the way required under its national legislation. Even in the case where the complaint receiving SA is the LSA, its decision needs to be adopted under the procedure of paragraph 8 as derogation from paragraph 7 (lex specialis rule). Therefore, the complaint receiving

SA adopting the decision may be either the LSA, another CSA, or both (or all), depending on the number and nature of complaint(s).

237. When the complaint is lodged with one, or more CSAs, the LSA shall prepare the draft decision dismissing/rejecting the complaint(s), and the CSAs shall issue a final decision in the EDPB Information System, adopting it also at national level and introducing the necessary national legal provisions.

238. The CSA, when issuing a decision, must give full effect to the draft decision, which is binding on LSA and other CSAs under Article 60(6) and/or the EDPB binding decision following Article 65(1)(a)⁹¹.

10.4 Inform and notify

239. Once the decision has been adopted, the complaint receiving SA(s) shall notify the complainant and inform the controller/processor⁹². This is to be done by each complaint receiving SA(s) according to their own national laws and practices and in the language provided by these provisions. For this purpose, the complaint receiving SA(s) may rely on the assistance of the LSA to inform the controller/processor on its behalf. In any case, the complaint receiving SA(s) needs to inform both the complainant and the controller about their possibility to seek judicial remedy in its MS.

240. The complaint receiving SA should then inform the other CSAs and the Board, including a summary of the relevant facts and grounds, as explained in section 9.4. This is grounded in the rationale of the information obligation mentioned in Article 60(7) regarding the decision adopted by the LSA, which is to ensure consistency by informing the other CSAs and the Board as a whole. The exchange of information on the actual decision finally adopted at national level – regardless of the SA that adopts such final national decision - is meant to ensure mutual knowledge of national decisions and avoid the arising of inconsistencies in the implementation of EU law. Thus, it would appear that although Article 60(8) does not explicitly require the CSA to provide a summary of the relevant facts and grounds, this is an overarching requirement that is intended to ensure consistent enforcement of the GDPR.

11 ARTICLE 60(9) – PARTIAL DISMISSAL/REJECTION

241. Article 60(9) is mainly a procedural step of the Article 60 procedure, which applies once the involved SAs have agreed on, and are bound by, a draft decision that contains both parts that were acted upon, and parts that were rejected/dismissed⁹³.

242. In practice, this means that, at this point of the procedure, the decision on partial dismissal/rejection will have already been taken, and the parts in the draft decision that relate to the dismissal/rejection and those that refer to further action by the LSA have been clearly marked in the draft decision. SAs now only need to formalise it through the necessary adoption procedures described in Article 60(9). This gives rise to final national decisions, which must give full effect to the draft decision, which is binding on all CSAs under Article 60(6) and/or the EDPB binding decision following Article 65(1)(a).

243. Accordingly, the related notification/information duties are split between the LSA and the complaint receiving SAs. The LSA adopts a decision for the parts of the complaint that were neither dismissed nor

⁹¹ The scope of possible changes is outlined in para. 207.

⁹² See section 10.4 on the difference between notifying and informing.

⁹³ See section 10.2 The meaning of these concepts is the same for both para.

rejected in line with what has been set forth in section 10.2. The LSA notifies its decision to the controller and informs the complainant about it; in this regard, the EDPB considers that the LSA may rely on the complaint receiving SA(s) to convey such information to the complainant(s) for the sake of administrative efficiency. Each complaint receiving SA(s) adopts a decision for the parts that were rejected/dismissed concerning the complaint that was submitted to it, following the approach laid out in the previous section (see, in particular, paragraph 239).

Example 14: Unhappy customer submits a complaint to its local SA, arguing that her data are kept and processed unlawfully by HappyCompany, which is infringing her rights. After performing the preliminary vetting the complaint is transferred to the LSA. The LSA starts an investigation and is informed by controller that indeed the complainant's data are kept in their files on account of a failure in their customer resource management that did not erase the unnecessary information in due time (preferences, purchase history, etc.). However, certain complainant's data have to be stored for longer because of financial and taxation requirements; proof of this is provided to the LSA. Therefore, the LSA shares a draft decision where it acts on parts of the complaint ordering the controller to finally erase the unnecessary information, and imposing a reprimand on the controller, but acknowledging the controller's right to keep the remaining personal data as required by law and the need for the complaint receiving SA to reject that part of the complaint. As no objection is raised, the LSA adopts a final national decision ordering the controller to comply with the complainant's request as for erasing the unnecessary information, notifies it to the controller and informs the complainant thereof; the complaint receiving SA adopts a final national decision rejecting the complaint as for the request to erase the necessary information and notifies it to the complainant, informing the controller thereof. The LSA and CSA will provide a summary of the relevant facts and grounds to the other SAs and the Board via the EDPB Information System, each of them for the respective final national decisions.

12 ARTICLE 60(10) – NOTIFICATION OF THE MEASURES ADOPTED BY THE CONTROLLER OR PROCESSOR TO THE LSA/CSA(S)

244. Paragraph (10) addresses the situation that occurs within the OSS mechanism and after a notification to the controller or processor of a decision adopted against it is made by the LSA requiring the controller or processor to act on the complaint.
245. This decision is notified as per either Article 60(7) or (9), when the LSA acts only on some of the grievances included in the complaint against the controller or processor.
246. The first sentence of Article 60(10) includes the obligation on the controller or processor to adopt the necessary measures to guarantee compliance with the decision, which applies the corrective powers granted in Article 58(2).
247. The controller or processor is obliged to ensure that these measures are implemented by all of its establishments in the EEA, where the processing at issue takes place.
248. The Article 60(10)(2) includes a second obligation for the controller or processor, i.e. to notify the LSA of any measures it has adopted to comply with the decision, where the latter entailed corrective

measures. This obligation ensures the effectiveness of the enforcement. It is also the basis of possible necessary follow-up actions to be commenced by the LSA, also in cooperation with the other CSAs⁹⁴.

249. The second sentence of Article 60(10) also includes an obligation for the LSA to inform the other CSAs of the measures adopted by the controller or processor to comply with the decision taken against it. Although there is no set deadline for the LSA to provide such information to the other CSAs, such information should be disclosed as soon as the LSA receives the information from the controller or processor.

When informing the other CSAs, the LSA should consider providing as well its assessment if it concludes that the measures taken are insufficient, in particular in order to decide whether further actions are necessary.

13 ARTICLE 60(11) – URGENCY PROCEDURE

250. Article 60(11) addresses the “*exceptional circumstances*” under which a SA may rely on the urgency procedure of Article 66 in the course of an Article 60 procedure.

251. For the purposes of these Guidelines, the focus will accordingly be mainly on the wording of Article 60(11), i.e. on the conditions for invoking Article 66 in the course of an OSS procedure, and on the consequences, this has on the ongoing OSS procedure.

13.1 The conditions for invoking Article 66

252. The following **cumulative** conditions must be fulfilled for a SA to invoke the urgency procedure under Article 66 pursuant to Article 60(11):

- The SA is a supervisory authority concerned;
- There are exceptional circumstances;
- The CSA considers that there is an urgent need to act; and
- Such urgency aims at protecting the interests of data subjects.

Explanations on each condition are provided below.

253. Article 60(11) refers to the CSA as part of an Article 60 procedure, i.e. to a CSA that participates in an OSS procedure⁹⁵. Such a CSA may invoke Article 66 if all the applicable conditions are fulfilled. Since the LSA is also a CSA according to the definition in Article 4(22), in principle an LSA may also invoke Article 60(11) if all the other conditions are fulfilled.

254. On the concept of “*exceptional circumstances*”, they could exist in situations where the urgency of the situation at hand is such as not to enable the use of the ‘standard’ cooperation or consistency procedures in a timeframe that is fitting. The exceptional nature of such circumstances dictates a restrictive interpretation. This applies in particular if, in spite of an ongoing Article 60 procedure, the CSA intends to request the EDPB, in accordance with Article 60(11), to adopt an urgent opinion or an

⁹⁴ See section 4.

⁹⁵ See para. 22 et seq.

urgent binding decision under the terms of Article 66(3) – i.e. when it is considered that a competent SA (most likely the LSA as such) “*has not taken an appropriate measure*”. All attempts by an SA to informally obtain an intervention from the competent SA should be made beforehand, and this is clearly also in line with the consensus objective underlying the whole Article 60 procedure.

255. On the “*urgent need to act*” and the criteria to be applied by the CSA to assess urgency under the specific circumstances, reference can be made to Recital 137, which states that this is in particular the case “*when the danger exists that the enforcement of a right of a data subject could be considerably impeded*”. According to European case law, it is not necessary for the imminence of the harm to be demonstrated with absolute certainty: it is sufficient to show that the damage is foreseeable with a sufficient degree of probability⁹⁶.

256. On the fourth condition, it should be pointed out that Article 60(11) does not refer to “*the rights and freedoms of data subjects*”, contrary to Article 66, but more broadly to their “*interests*”. However, since the procedure to be applied is the one “*referred to in Article 66*”, the EDPB considers that such interests do coincide with the rights and freedoms of data subjects as per Article 66.

257. As mentioned above, these conditions are cumulative and it is the responsibility of the CSA to provide “*reasons*” for each of them, regardless of whether it intends to take urgent measures under Article 66(1) or request an urgent opinion or an urgent binding decision from the EDPB under Article 66(2) or (3).

258. Furthermore, a CSA should consider several additional factors on top of the conditions set forth in Article 60(11) prior to taking such a step e.g.:

- the elements gathered from the OSS procedure,
- exchanges with the other CSAs (including the LSA),
- exchanges with the controller/processor and, where applicable, the complainant regarding the cross-border processing at issue,
- the stage reached within the Article 60 procedure (in particular, how close the procedure is to its finalization, and therefore to the taking of enforcement action regarding the controller/processor).

259. Concerning the “*urgent need to act*”, the CSA should in particular take account of the last point.

[**13.2 The interaction with an ongoing Article 60 cooperation procedure**](#)

260. The urgency procedure under Article 66 derogates from the Article 60 procedure due to its exceptional nature; however, it leaves it unprejudiced. Thus, if a CSA relies on an urgency procedure in accordance with Article 60(11), and all the relevant conditions are fulfilled, it does not have the effect of terminating the existing OSS procedure. Therefore, the consequences resulting from the adoption of provisional measures by the CSA under Article 66(1)), and/or of an urgent opinion or binding decision requested by the EDPB under Article 66(2) or (3), will have to be factored in that OSS procedure accordingly.

⁹⁶ See order in Case T-346/06 R IMS v Commission [2007] ECR II-1781, paragraphs 121 and 123.

261. From a general standpoint, a distinction can be drawn depending on the nature of the urgent measures sought:

- the CSA adopted measures that are provisional and limited in time and to its national territory pursuant to Article 66(1) and does not intend to request final measures to the EDPB;
- the CSA adopted provisional measures under Article 66(1) and intends to obtain final measures via the application of Article 66(2), or the CSA intends to directly obtain final measures via the application of Article 66(3);

262. In the case of application of Article 66(1), the OSS procedure can continue towards the adoption of final measures under the LSA's direction, without the CSA's provisional measures having any particular consequences on the OSS procedure. In the scenario where Article 66(2) or (3) is applied, the urgent measures requested to the EDPB by the CSA are final in nature. Hence, in such scenario, the urgent binding decision or urgent opinion adopted by the EDPB is bound to impact the ongoing OSS procedure, in particular on account of the need for the LSA to implement it without delay. Accordingly, the LSA and other CSAs will have to suspend the handling of the case pending the issuance of such urgent binding decision or urgent opinion.

263. Once the EDPB issues its urgent opinion or urgent binding decision, the OSS procedure can recommence and the effects produced by the urgency procedure will have to be factored in the OSS procedure. However, it should be considered that the LSA is required to adopt its final decision in pursuance of such EDPB urgent opinion or urgent binding decision within a very limited timeframe set by the EDPB on case-by-case basis (e.g. two weeks or one month), exactly on account of the urgency of the matter as endorsed by the EDPB.

264. The LSA and the other CSAs are in the best position to establish whether the issues addressed by the ongoing OSS procedure have been fully covered by the LSA's final decision adopted on the basis of the EDPB's urgent binding decision or urgent opinion, or if there are outstanding issues.

265. In the former case, the OSS procedure will come to its conclusion following the adoption of the final decision by the LSA, which will be followed by the procedural steps regulated under the terms of Article 60(7-9) as the case may be. This may mean that, since the matter is closed, no draft decision will be shared by the LSA in accordance with Article 60(3)⁹⁷. If there are further issues that need to be addressed on top of those that have been the subject of the urgent opinion or urgent binding decision, the LSA will have to clearly identify which issues part of its draft decision remain to be addressed within the current OSS procedure and which ones were resolved via the urgent binding decision or urgent opinion adopted by the EDPB. In such a case, the current Article 60 procedure will resume after the LSA adopted and notified its final decision, from the stage at which it was suspended because of the urgency procedure.

⁹⁷ In any case, the views of the other CSAs were already expressed via the urgent binding decision or urgent opinion adopted by the EDPB.

QUICK REFERENCE GUIDE

I. INTRODUCTION

This annex is based on the GDPR and the Article 60 guidelines of the EDPB and should be read with the relevant sections of them for any question of legal interpretation.

This document is meant to provide quick reference information on the procedures relating to the Cooperation between the lead Supervisory Authority (LSA) and the other Supervisory Authorities concerned (CSA) in case of cross border processing. Accordingly, the document is structured in accordance with the sequence of the steps to be performed in an Article 60 procedure by highlighting both legal obligations and shared best practices as set out in the said GDL.

As for the phase prior to the starting of an Art. 60 procedure, in particular regarding determination of the LSA and preliminary vetting of cases, reference should be made to WP244 rev.01 and to the other relevant guidance.

The main phases in an OSS procedure are outlined below:

PHASE 0: decide who is LEAD

This is related to the confirmation that cross-border processing takes place and the location of the main or of the single establishment of the controller/processor (Art. 56)

PHASE I: exchange relevant information and investigate

Art. 60 (1)

Possibly Art. 60 (2):

mutual assistance & joint operations

PHASE II: prepare decision

Art. 60(3) to (5)

PHASE III: adopt decision

Art. 60 (6) to (10)

Possibly Art. 60 (2):
mutual assistance & joint operations

EDPB
Information
System
Art. 60(12)

II. STEP BY STEP PROCEDURE

Phase I: Exchange information & Investigate

	Legal Requirements	Who, When and What	Recommendations and best practices	EDPB Information System (IMI)
1a	Article 60(1) – <i>The lead supervisory authority shall cooperate with the other supervisory authorities concerned (...) in an endeavor to reach consensus. (...)</i>	<p>Who: LSA and CSA equally</p> <p>When: throughout the entire cooperation procedure</p> <p>What:</p> <ul style="list-style-type: none"> - Mandatory cooperation - Active cooperation (fair and constructive) to prevent disputes in an endeavour to reach consensus (42) 	<ul style="list-style-type: none"> - Utmost and determined effort by SAs to achieve consensus as a legal objective (39); - Consensual acting should be the rule (41); - Use all possible tools to reach consensus (40,42); - Select cooperation approaches best suited for the case at hand (43); - Provide each other the opportunity to express its views (42); - Take each other's views into account (42, 127). 	
1b	Article 60(1) – <i>(...) The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.</i>	<p>Who: LSA and CSA equally</p> <p>When: throughout the entire cooperation procedure, in a timely manner</p> <p>What:</p> <ul style="list-style-type: none"> - Mandatory exchange of all relevant information on the subject matter - Exchange of necessary documents and views before the submission of the draft decision 	<ul style="list-style-type: none"> - Exchange all information (facts and legal reasoning) necessary to reach a conclusion on the case (46); - Informal exchanges among SAs in earlier stages and raising of possible issues, before triggering formal steps, to increase the likelihood of reaching consensus (55-57); - Information exchanges should be adequate and proportionate to enable SAs to perform their role (47); - For the LSA: relevant information when dealing with the controller/processor (findings, 	<i>Art 60 Informal Consultation</i>

	Legal Requirements	Who, When and What	Recommendations and best practices	EDPB Information System (IMI)
			<p>reports, exchanges with the organization) (48-50);</p> <ul style="list-style-type: none"> - For the CSA: relevant information regarding the case (complaint, further correspondence, data breach notification, any further findings, etc.) (50); - Only share personal data if necessary to deal with the case (51); - Flag specific issues as confidential to meet national legal requirements (52). 	
2	<p>Article 60(2) – The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 (...) in particular for carrying out investigations (...)</p>	<p>Who: LSA</p> <p>When: at any time prior to submission of DD</p> <p>What:</p> <ul style="list-style-type: none"> - Possibility to request mutual assistance to a CSA(s), including to investigate an ongoing cross border case. - Such requests follow the rules of Article 61 (grounds for the request; deadlines for the reply). - Reply by CSAs without undue delay and no later than 1 month after receiving the request. 	<ul style="list-style-type: none"> - Requests can cover: additional info from the complainant; facts to be checked; evidence to be collected; inspections to be carried out on the establishment of the controller/processor (70-73). 	<p>Art 61 Mutual Assistance Art 61 Voluntary Mutual Assistance</p>

	Legal Requirements	Who, When and What	Recommendations and best practices	EDPB Information System (IMI)
3	<i>Article 60(2) – The lead supervisory authority (...) may conduct joint operations pursuant to Article 62, in particular for carrying out investigations (...).</i>	<p>Who: LSA</p> <p>When: at any time prior to submission of the DD</p> <p>What:</p> <ul style="list-style-type: none"> - Possibility to set up a joint operation to investigate a controller or processor established in another Member State - Rules of Article 62 are applicable to such joint operation 	<ul style="list-style-type: none"> - The joint operation can be hosted by the LSA or can be organized by the LSA and deployed in one or several Member States where there are establishments of the controller/processor relevant for the specific case (79-80). <p>NOTE: Article 60(2) may also be relied on after conclusion of the OSS procedure to perform checks under 60(10) (see below) (74, 80).</p>	<p><i>Art 60 Informal Consultation</i></p> <p><i>Art 62 Joint Operation</i></p>

Phase II: Prepare decision

	Legal Requirements	Who, When and what	Recommendations and best practices	IMI
1a	Article 60(3) – The LSA shall, without delay, communicate the relevant information on the matter to the other supervisory authorities.	<p>Who: LSA</p> <p>When: without delay</p> <p>What:</p> <ul style="list-style-type: none"> - Communicate to the CSAs the relevant information on the case at hand 	<ul style="list-style-type: none"> - Information to be provided to the CSAs swiftly, according to the circumstances of the specific case (87-88); - The LSA should consider to proactively and quickly share a timetable with the steps to be taken until the submission of the draft decision (89-90, 102); - After completion of investigation, the LSA should send a summary of the results to the CSAs for their feedback within a short reasonable deadline. The LSA shares its assessment on the feedback received (94); - ‘Relevant information’ includes any additional exchanges on controversial issues or divergent views in line with the consensus objective (93-95); - The LSA can share with the other CSAs the scope and main conclusions of the DD prior to its formal submission, in order for the CSAs to contribute to the overall procedure (57, 93); - In the preparation of the DD, the LSA should take into account the views 	Art 60 Informal Consultation

	Legal Requirements	Who, When and what	Recommendations and best practices	IMI
			<p>preliminarily expressed by the CSAs (93-94);</p> <ul style="list-style-type: none"> - In simple cases, where the DD is self-explanatory and/or very little information needs to be exchanged, the relevant information may only be shared along with the DD (104). <p>NOTE: See Phase 1, step 1b</p>	
1b	<p>Article 60(3) – It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion (...)</p>	<p>Who: LSA</p> <p>When: as soon as possible, after gathering all facts and exchanging information and points of view with the CSAs, which depends on the complexity and particularities of cases.</p> <p>What:</p> <ul style="list-style-type: none"> - Mandatory submission of a draft decision to the CSAs in all Article 60 cases for consultation purposes. 	<ul style="list-style-type: none"> - The submission of a DD applies to all OSS procedures, including in situations where: the complaint is withdrawn during an ongoing A60 procedure; there is an amicable settlement; the infringement ceased; the case is to be closed; no action against the controller or processor is envisaged; or where the LSA is not issuing the final decision (97-100); - The DD should correspond in form and content to the decision to be adopted in the specific case, and contain all formal requirements of a legally binding measure (109-110, 114-117); - The DD should have a written form, clear and unambiguous wording, 	Art 60 Draft Decision

	Legal Requirements	Who, When and what	Recommendations and best practices	IMI
		<p>further submissions from the controller/processor, the LSA may withdraw its draft decision within the 4-week period consultation envisaged under 60(4), clearly stating its reasons, and submit a new DD to the CSA(s), as swiftly as possible, and a new deadline starts running (163).</p>	<p>issuing SA, date of issue, signature of authorized SA staff, reference to the right to an effective remedy (109);</p> <ul style="list-style-type: none"> - The draft decision should also contain a description of relevant facts, sound reasoning and a proper legal assessment, so CSAs fully understand its conclusions (104, 111,113); - The DD should set out clearly whether an issuing under Art 60(7), (8) or (9) is pursued. In case of Art 60(9) it should be clear what will be issued by the LSA and what by the complaint receiving SA(s) (227); - The four-week period starts running upon submission of the DD (103,135); - The LSA should ensure that only triggers the workflow in working days and that the deadline does not expire on an EU holiday (138). - The LSA should make sure the DD is fully compliant with the national rules for the right to be heard (RTBH), and that the steps taken in that regard are referenced in the DD (105). 	
1c	Article 60(3) – [The LSA shall] take due account of their views	Who: LSA	<ul style="list-style-type: none"> - The LSA should react to the views provided by all CSAs (129); 	

	Legal Requirements	Who, When and what	Recommendations and best practices	IMI
		<p>When: as swiftly as possible</p> <p>What:</p> <ul style="list-style-type: none"> - Consider the views of CSAs regarding the draft decision, in order to reach a consensual outcome. 	<ul style="list-style-type: none"> - The LSA should explain how it intends to take due account of such views, which are to be followed and those which are not, including for being contradictory among each other (129); - The LSA should take the utmost account of the views of the complaint receiving CSA, since it acts as a point of contact for the complainant and this CSA may be required to adopt and defend a decision (130). <p>NOTE: See Phase I, step 1a, on reaching consensus and Phase II, step 1a, on the preparation of the draft decision</p>	
2a	<p>Article 60(4) – <i>Where any other of the CSAs within a period of four weeks after being consulted (...) expresses a relevant and reasoned objection to the draft decision, (...)</i></p>	<p>Who: CSA(s) recognized as participating in the OSS procedure</p> <p>When: Within 4-week period following submission of DD by LSA</p> <p>What: Option to submit a RRO on the DD.</p> <p>NOTE: See EDPB Guidelines 9/2020 on concept of RRO</p>	<ul style="list-style-type: none"> - Reaching consensus should take priority over initiating the dispute resolution process, so previous steps should be carefully followed (133); - The CSA should provide its objection(s) in one single submission, though distinguishing the different objections (139); - If the CSA wishes to modify its submission, it can still do so during the 4-week period by deleting the previous version and uploading in IMI a new one (139); 	Art 60 Draft Decision

	Legal Requirements	Who, When and what	Recommendations and best practices	IMI
			<ul style="list-style-type: none"> - An endorsement or referral to another CSA's objection does not constitute a RRO. Each CSA should then submit its own objection complying with the RRO guidelines (142-145). 	
2b	<p><i>(...) the LSA shall, if it does not follow the RRO or is the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism</i></p>	<p>Who: LSA</p> <p>When: as soon as possible, after the 4-week period of consultation on the DD</p> <p>What:</p> <ul style="list-style-type: none"> - Mandatory submission of matter of the case to EDPB under Article 65(1)(a) if LSA does not follow RRO/does not find objection to be a RRO <p>NOTE: See EDPB Guidelines 9/2020 on concept of RRO</p>	<ul style="list-style-type: none"> - Reaching consensus should take priority over initiating the dispute resolution process, so previous steps should be carefully followed (133,149); - In response to RRO, the LSA should convey its first assessment and present which RRO intends to follow and in what extent, and which does not, and better clarify its position while giving the CSA(s) the opportunity to further explain the objections (146-149); - Such additional cooperation can take different forms, including organization of meetings or use of informal consultation procedures (146, 159); - Following the LSA's explanations and if the conflicting views are only marginal, the CSA(s) may consider withdrawing the RRO. In such situation, the CSA should explicitly declare that it withdraws its RRO (147-149); 	<i>Art 65 - Dispute Resolution by the Board</i>

	Legal Requirements	Who, When and what	Recommendations and best practices	IMI
			<ul style="list-style-type: none"> - The LSA should document this withdrawal and notify the other CSA(s) without delay (148); - When consensus is not achieved, the LSA should refer the matter to the EDPB as soon as possible 151-153, 174, 181). <p>NOTE: If the LSA wishes to follow some objections, but does not wish to follow other objections and/or does not consider them to be relevant and/or reasoned, the LSA should submit a revised draft in the procedure as per Article 60(5), according to the following section. →The LSA should indicate clearly, through an informal exchange, which of the objections it intends to follow within the revised draft decision and how it intends to do so. Further, the LSA should indicate clearly, which objections have been noted as being the subject of a possible later dispute resolution via Article 65(1)(a) (154).</p>	

3a	<p>Article 60(5) – Where the LSA intends to follow the RRO, it shall submit to the other CSA a revised draft decision for their opinion.</p>	<p>Who: LSA</p> <p>When: as soon as possible (good administration principle)</p> <p>What:</p> <ul style="list-style-type: none"> - Mandatory submission of a revised draft decision to the CSA(s), only in case the LSA intends to follow a RRO. <p>NOTE: See Phase II, step 1b, on submission of the draft decision</p>	<ul style="list-style-type: none"> - The LSA is barred from submitting a revised draft decision solely on account of comments or other remarks (162-163 and EDPB Guidelines 9/2020); - Following the assessment of the RRO, the LSA should clearly state to all CSA(s) its intention to submit a revised draft decision (RDD) (169-170); - The lapse of time between the RRO and the submission of a RDD should be as small as possible and appropriate to the OSS procedure (167-168); - Prior to the formal submission, the LSA may share a preliminary RDD, via informal consultation, to ensure that there is agreement on the amendments introduced and consensus can be achieved (170); - The RDD should completely address the risks posed by the initial DD regarding the data subjects' fundamental rights and freedoms, as identified in the RRO (158). 	<p>Art 60 Revised Draft Decision</p>
----	-----------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------

	Legal Requirements	Who, When and what	Recommendations and best practices	IMI
3b	<i>Article 60(5) – (...) That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks</i>	<p>Who: LSA and CSA(s) recognized as participating in the OSS procedure</p> <p>When: See Step 2a/2b in Phase II</p> <p>What: See Step 2a/2b in Phase II</p> <p>NOTE: In case no RROs are raised, article 60(6) applies</p>	<ul style="list-style-type: none"> - The RDD should be regarded as a different legal instrument compared to the DD submitted under 60(4) (183); - A CSA may raise a RRO to the RDD even if it had not raised an objection to the DD (183-184); - A CSA should not raise a RRO in relation to a RDD if there was no RRO directed at that specific issue and the LSA has not revised the draft decision in respect of such issue (186). <p>NOTE: See Phase II, Step 2a/2b on the submission of RRO</p> <hr/> <p>EXCEPTIONAL CASE: If there are extraordinary circumstances, not met before, where the LSA mindfully intends to follow a RRO raised during this last consultation period that allows reaching consensus and avoiding to refer the matter to the EDPB when there is no longer a dispute to be settled, the LSA may submit a (re) revised draft decision (176-180).</p>	Art 60 Revised Draft Decision

Phase III: Adoption of final decision

	Legal Requirements	Who, When and What	Recommendations and best practices	IMI
1	<p>Article 60(6) - Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.</p>	<p>Who: The CSA(s) recognized as participating in the OSS procedure</p> <p>When: After 4 weeks from submission of DD (60.4); or after 2 weeks from submission of (last) RDD (60.5)</p> <p>What:</p> <ul style="list-style-type: none"> - Agreement between LSA and CSA on DD/RDD, in the absence of RROs - Bindingness of DD/RDD on LSA and CSAs → DD/RDD may no longer be withdrawn or amended, subject to exceptional circumstances. (187; 191) 	<ul style="list-style-type: none"> - No need to act, agreement is implied by absence of RROs (tacit agreement) (188) - National final decision by LSA/CSA [see 2a/2b] should not depart from binding DD/RDD (189-191) - Binding effect limited to specific, concrete case addressed (196) - A CSA intending to join the procedure at this stage should consider initiating a separate OSS procedure (otherwise, it will be automatically bound by DD/RDD). (192-195) - Text/Conclusions of binding DD/RDD may be re-used for subsequent OSS procedure (same or different controller, same infringement) if this can speed up handling of case. (197-198) 	
2a	<p>Article 60(7) – (I) The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities</p>	<p>Who: The LSA</p> <p>When: As swiftly as possible from bindingness under 60(6) (good administration principle) (206) / NOTE: within 1 month from EDPB binding decision under 65(1)(a) (206)</p>	<ul style="list-style-type: none"> - Provide full copy of final national decision (as per national law) to controller/processor (210) - Inform controller/processor also on their obligations under 60(10) (214) - Use IMI “Final Decision” fields to inform other CSAs and EDPB of national final decision (211-212) 	Art 60 Final Decision

	Legal Requirements	Who, When and What	Recommendations and best practices	IMI
	<i>concerned and the Board of the decision in question, including a summary of the relevant facts and grounds.</i>	<p>EXCEPTIONAL CASE: Supervening constraints during this period (e.g. relevant EU case law/legislation) may require LSA to refrain from adopting national final decision and to submit new DD to CSAs, after informing CSAs (207)</p> <p>What:</p> <ul style="list-style-type: none"> - Adoption of the national final decision (203-205; 230-235) - Notification of national final decision to establishment of controller/processor (pursuant to national law) (208-209) - Information to other CSAs and Board about national final decision - Summary of facts and grounds in decision 	<ul style="list-style-type: none"> - Use IMI "Final Decision" fields to provide summary of facts and grounds to other CSAs and EDPB (215-216) - A copy of national final decision in English is also recommended to be provided to CSAs, via IMI (217) 	
2b	Article 60(7) – (II) The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.	Who: The CSA which received a complaint addressed in the binding decision under 60(6) or 65(1)a, in which action is taken by the LSA on the complaint	<ul style="list-style-type: none"> - Information should be provided to complainant in line with national law and practices (213) - Complainant should be informed that right of redress (if any) is to be exercised in the LSA's MS (national law) (213) 	Art 60 Final Decision

	Legal Requirements	Who, When and What	Recommendations and best practices	IMI
		<p>When: As swiftly as possible (good administration principle) following information by LSA on adoption of national final decision</p> <p>What: Information to complainant on national final decision adopted by LSA</p>		
3	<p>Article 60(8) - By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof</p>	<p>Who: The CSA which received a complaint addressed in the binding decision under 60(6) or 65(1)a, if the complaint is dismissed or rejected (218-219; 236-238)</p> <p>When: As swiftly as possible (good administration principle) following bindingness under 60(6) / within one month following bindingness under 65(1)a</p> <p>What:</p> <ul style="list-style-type: none"> - Adoption of national final decision dismissing/rejecting complaint (national law) (221-225; 228-229) - Notification of national final decision to complainant (national law) (219; 226) 	<ul style="list-style-type: none"> - The CSA may rely on LSA to convey information on national final decision to controller/processor (239) - Use IMI "Final Decision" fields to inform other CSAs and EDPB of national final decision (240) - Use IMI "Final Decision" fields to provide summary of facts and grounds to other CSAs and EDPB (240) - Controller/processor should be informed that right of redress (if any) is to be exercised in the CSA's MS (national law) (239) - A copy of national final decision in English may be also provided to CSAs, via IMI (240) 	Art 60 Final Decision

	Legal Requirements	Who, When and What	Recommendations and best practices	IMI
		<ul style="list-style-type: none"> - Information to controller on national final decision (national law) (220) - Information to other CSAs and Board about national final decision - Summary of facts and grounds in decision 		
4a	<p>Article 60(9) – (I) <i>Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter.</i></p>	<p>Who: LSA and CSA bound by agreement (under 60(6)) / bound by decision (under 65(1)a) to partly dismiss/reject and partly act on a complaint (241-242)</p> <p>When: As swiftly as possible (good administration principle) following bindingness under 60(6) / within one month following bindingness under 65(1)a</p> <p>What:</p> <ul style="list-style-type: none"> - Adoption of separate national final decisions by LSA and CSA regarding different outcomes in respect of the same complaint (242) 		

	Legal Requirements	Who, When and What	Recommendations and best practices	IMI
4b	Article 60(9) – (II) <i>The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof</i>	Who: The LSA taking action on part of a complaint in relation to the controller When / What: See Step 2a for LSA NOTE: The LSA must inform complainant of the national final decision it has adopted (243)	See Step 2a for LSA NOTE: The LSA may rely on CSA to convey information on national final decision to complainant (243)	Art 60 Final Decision
4c	Article 60(9) – (III)[...] <i>the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof</i>	Who: The CSA dismissing or rejecting part of a complaint When / What: See Step 3 for CSA	See Step 3 for CSA	Art 60 Final Decision
5a	Article 60(10) – (I) <i>After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union.</i>	Who: Controller/processor When: After notification by LSA of national final decision under 60(7) or 60(9) (244-245) What: Taking and notification of measures to ensure compliance with		

	Legal Requirements	Who, When and What	Recommendations and best practices	IMI
5b	Article 60(10) – (IIa) <i>The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority [...]</i>	LSA's national final decision (243; 246-248)		
5c	Article 60(10) – (IIb) <i>[the lead supervisory authority], which shall inform the other supervisory authorities concerned.</i>	<p>Who: The LSA</p> <p>When: As soon as possible following notification by controller/processor (249)</p> <p>What: Information to CSAs on measures taken by controller/processor</p>	<ul style="list-style-type: none"> - LSA should consider providing CSAs with assessment of measures taken by controller/processor (249) - LSA may request mutual assistance from CSAs under 60(2) to verify compliance by controller/processor in relevant establishments (62; 69; 74; 80) 	

ARTICLE 60(11) – URGENCY PROCEDURE

	Requirements	Who, When and What	Recommendations and best practices	IMI
U	<p>Article 11 - Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply</p>	<p>Who: CSAs and LSA</p> <p>When: At any time in the course of an OSS procedure, if exceptional circumstances apply</p> <p>What: Application of urgency procedure under Article 66</p> <p>NOTE: EDPB binding decision in urgency procedure under 66(3) may entail adoption of national final decision without DD/RDD (265)</p>	<ul style="list-style-type: none"> - SAs should consider various factors, in particular the stage reached in OSS procedure, prior to invoking urgent need to act (252-259) - CSAs and LSAs should jointly consider how best to factor the outcome of the Article 66 procedure into the ongoing OSS procedure (260-265) 	<p>Art 66 Adopted Provisional Measures</p> <p>Art 66 Urgent Opinion/Decision by the EDPB</p>

Internal EDPB Documents



Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR

Version 2.0

Adopted on 14 May 2019

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Version history

Version 2.0	15 December 2020	Review of the guidelines
Version 1.0	14 May 2019	Adoption of the guidelines

Table of contents

1	PART 1 - INTRODUCTION.....	4
2	PART 2 – STEPS TO HANDLE A CASE UNDER ARTICLE 56.2 GDPR	5
2.1	Analysis of the case by the receiving supervisory authority	5
2.1.1	Determine if the case relates to cross-border processing	5
2.1.2	Determine if the cross-border case falls under Article 56.2	7
2.1.2.1	The subject matter of the complaint or the infringement relates only to one establishment in the Member State of the supervisory authority	8
2.1.2.2	The subject matter of the complaint or the infringement substantially affects data subjects only in its Member State	8
2.1.2.3	The case is about an infringement of only national legislation.....	10
2.2	Informing the lead supervisory authority	10
2.3	Decision of the lead supervisory authority under Article 56.3	11
2.3.1	How does the LSA choose to handle the case or not?.....	11
2.3.1.1	The presence of an establishment of the controller or processor in the supervisory authority's Member State	11
2.3.1.2	Whether the case raises a new matter of principle	12
2.3.1.3	Other criterion.....	13
2.3.2	The LSA informs the supervisory authority of its decision to handle the case or not ..	13
2.3.3	What can be done when the LSA has not informed the supervisory authority of its choice during the period of three weeks?	14
2.4	The Lead supervisory authority handles the case under Article 56.4.....	14
2.5	The receiving supervisory authority handles the case under Article 56.5	15
2.5.1	The supervisory authority is competent to handle the case and use cooperation measures	15
2.5.2	How and by whom is a binding decision imposed to the controller or the processor?	16
2.6	Informing the complainant.....	16
2.7	Handling a case by the lead supervisory authority under Article 56.2	17
	Annex: Flowchart.....	18

The European Data Protection Board

Having regard to Article 70 (1) (e) and 56.2 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

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

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018,

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 PART 1 - INTRODUCTION

1. The general rule in the GDPR is that the cross-border processing is assessed by means of the cooperation of the lead supervisory authority (LSA) and the supervisory authorities concerned (SAC).
2. Indeed, according to Article 56.1 of the GDPR, a supervisory authority (SA) is competent to act as a LSA for the cross-border processing carried out by a controller or a processor which has its main or its only establishment in its Member State¹.
3. Article 56.2 covers cases that are derogations to the general rule: the cases involving cross-border processing but which have only local impacts in the Member State of the supervisory authority where the complaint was first lodged or that first detected a possible infringement.
4. For such cases with only local impacts, Articles 56.2 and 56.3 provide that the supervisory authority which received the complaint or was made aware of a possible infringement shall be competent if the LSA decides not to handle the case. As Article 56.2 lays down a derogation, these provisions must be given a strict interpretation. The present internal guidance aim to identify the scope of cases that come under this exception and to set up common handling procedures.
5. It is also important to underline that Article 56 does not apply to every case. Indeed, according to Article 55 of the GDPR, if the processing is carried out by public authorities or private bodies acting on the legal basis laid down by Articles 6.1.c and 6.1.e², the SA of the Member State concerned shall be competent and Article 56 does not apply.

¹ In such cases, the supervisory authority acts as lead supervisory authority.

² Article 6.1.c: "the processing is necessary for compliance with a legal obligation to which the controller is subject " ; Article 6.1.e: "the processing is necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller".

6. The procedural steps outlined in this guidance should be applied by supervisory authorities from the outset of handling any case that potentially relates to cross-border processing. For cases that clearly do not involve cross-border processing this guidance does not apply.
7. This guidance shall be read together with other documents adopted on cooperation among supervisory authorities under the GDPR (e.g. designation of Lead Supervisory Authority, one-stop-shop mechanism, mutual assistance and joint operations, territorial scope of the GDPR).

2 PART 2 – STEPS TO HANDLE A CASE UNDER ARTICLE 56.2 GDPR

8. Each supervisory authority that receives a complaint or detects an infringement is required to establish whether the case concerns a cross-border processing and whether it should be handled locally, according to the common definitions of these notions (2.1). Once the cross-border nature of the processing and the local nature of the case have been determined by the receiving SA, the handling procedures set out in this section (2.2 – 2.6) must be followed. A flowchart, providing a step-by-step guidance, is included in the annex of the present internal guidance.
9. A distinction is made between the reception of a complaint or the detection of an infringement by a supervisory authority (2.1 – 2.6) and by a lead supervisory authority (2.7).

2.1 Analysis of the case by the receiving supervisory authority

2.1.1 Determine if the case relates to cross-border processing

10. The condition for Article 56 to apply is that the processing at stake is cross-border in nature. If the processing is not cross-border in nature, the supervisory authority that receives the case is competent to handle it, if the processing is carried out in its Member State³.
11. Moreover, and as previously mentioned, according to Article 55 of the GDPR, if the processing is carried out by public authorities or private bodies acting on the basis of Articles 6.1.c and 6.1.e, the SA of the Member State concerned shall be competent and Article 56 does not apply.
12. In order to ascertain that the case at stake concerns a cross-border processing, the SA must verify if one of the two conditions laid down by Article 4(23) of the GDPR is fulfilled:
 -) The processing of personal data takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
 -) The processing of personal data 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 subjects⁴ in more than one Member State.

³ See point 27, second bullet, last sentence of the Internal EDPB Document 06 /2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints.

⁴ For the definition of “substantially affect, see WP 244 Guidelines for identifying a controller or processor’s lead supervisory authority, page 3. point I.

13. To determine if the first criterion applies, the information already gathered in the preliminary vetting phase will be helpful⁵. Indeed, the SA must determine the location of the controller or the processor's establishments⁶ within the European Economic Area's territory. It is not necessary that the processing in question is carried out "by" the EEA establishments themselves. Indeed, according to Article 4(23), the processing only has to be carried out "*in the context of the activities*" of these establishments⁷.
14. It is important to ensure that the processing mentioned in the case is cross-border and not a "national processing" that has to be handled according to Article 55 of the GDPR – a processing that takes place in the context of activities of an establishment situated in only one Member State and substantially affects or is likely to substantially affect data subjects only in that one Member State.

Example 1: National processing

The Polish supervisory authority receives a complaint from an employee of a Polish company, which is a branch of a Swedish company, about the handling of its Human resources data. The Polish SA using the preliminary vetting procedure⁸ determines that the data is processed by this company in Poland alone, and relates only to its Polish employees and any decision about the purposes and means of this processing is taken in Poland (the Human resources policy is also set in Poland and also the servers on which these data are held in Poland).

Although, there is a parent company in Sweden, the Polish Company is the controller of the Polish Human resources personal data and the Swedish Company has no role in the processing of these data. Since this complaint is not about cross-border processing, Article 56 of the GDPR does not apply and the Polish supervisory authority is fully competent to handle the case.

Example 2: National processing carried out in another Member State

The Polish supervisory authority receives a complaint from a Polish citizen who is a resident of Belgium and works for a company in Belgium, which is a branch of a Swedish company. The complaint is about the handling of its Human resources data. The data is processed by this company in Belgium alone, and relates only to its Belgian employees, and any decision about the purposes and means of this processing is taken in Belgium (the Human resources policy is set in Belgium and the servers on which these data are held are in Belgium).

Although, there is a parent company in Sweden, the Belgian company is the controller of the Belgian Human resources personal data and the Swedish company has no role in the processing of these data. Since this complaint is not about a cross-border processing, Article 56 of the GDPR does not apply.

Example 3: Cross-border processing

The Polish supervisory authority receives a complaint from an employee of a Polish company, which is a branch of a Swedish company, about the handling of its Human resources data for career advancement purposes. The data which are the object of the complaint is processed by this company in Poland and the servers on which these data are held are in Poland. However, the parent company which decides on purpose and means of the processing at issue is established in Sweden. As the Human

⁵ Internal EDPB Document 6/2000 on preliminary steps to handle a complaint: admissibility and vetting of complaints .

⁶ Recital 22 of the GDPR: "Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect".

⁷ For the definition of "an establishment in the Union" and "processing of personal carried out in the context of the activities of an establishment", see the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

⁸ Internal EDPB Document 6/2000 on « preliminary steps to handle a complaint: admissibility and vetting of complaints »

resources policy is set by the Swedish parent company for several of its establishments in the EEA (including Poland) where the same kind of processing takes place, the processing at issue (concerning human resources data) is a cross-border processing because it is carried out in the context of the activities of more than one establishment (including the Polish establishment) of the same controller (the Swedish company).

The complaint is related to a cross-border processing and the Polish SA should follow the next step to determine if the complaint may be considered as having only local impacts⁹.

15. Another situation that does not regard cross-border processing, within the meaning of the first criterion of Article 4(23) of the GDPR, is where the controller or processor has several establishments only outside of the European Economic Area (even if it processes personal data of data subjects who are in the Union).

Example 4

If a company, which offers goods or services to data subjects in one or more Member States has an establishment in the United States and another one in Japan, the processing at stake is not qualified as cross-border, and therefore cannot benefit from the one-stop-shop procedure. Then, if a supervisory authority receives a complaint about this processing, it can handle the case without applying Article 56.

16. Where the SA determines that the controller or processor has only one establishment in the Union, **it must verify if the second Article 4(23) criterion applies** to determine whether the case at stake concerns cross-border processing.

Example 5

If a single establishment in the Union offers a service through a website available in different European languages, even if it is not sufficient *per se*, this may indicate that data subjects in more than one Member State are substantially affected, or are likely to be substantially affected, by the processing carried out, which could characterize the processing as cross-border.

2.1.2 Determine if the cross-border case falls under Article 56.2

17. Once the SA has deemed that the case concerns cross-border processing, it should consider whether the case has only local impacts or not.
18. As already recalled, each supervisory authority is competent to handle a complaint lodged with it or a possible infringement of the GDPR about a cross-border processing, if the case's subject **matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State**.
19. The "subject matter of a case" refers to the specific conduct of the controller or processor as detected by the supervisory authority or alleged by the complainant that amounts to a possible infringement of one or more provisions of the GDPR.

⁹ Except where Article 55.2 of the GDPR applies.

2.1.2.1 The subject matter of the complaint or the infringement relates only to one establishment in the Member State of the supervisory authority

20. As a first step, the SA must verify the existence of an establishment¹⁰ of the controller or processor in its Member State and that the processing of personal data in question is carried out in the context of the activities of this establishment.
21. If there is such an establishment in its territory, the SA must determine whether the case's subject matter relates only to this establishment, regardless of the impact on data subjects caused by the processing at stake. In general terms, the fact that a subject matter relates only to one establishment means that it is about¹¹ that establishment.
22. The SA should establish whether, in a cross-border processing situation, the conduct of the controller or processor is such as to relate only to the establishment in its Member State.

Example 6

A retail company is established in several Member States. Due to repeated thefts occurring in the store located in France, the Italian headquarters decides to use of video surveillance, but only for the establishment located in France. The images are stored in Italy in the headquarters' offices. Since the Italian establishment determines the purposes and means of this monitoring system, this is a cross-border processing and the controller's main establishment is in Italy. If a French employee or a customer lodges a complaint within the French supervisory authority regarding the use of the surveillance-camera, the SA may find that this case relates only to the establishment in its Member State since no other establishment makes use of video-surveillance. If that is the case, the SA may handle the complaint locally, subject to the LSA's decision.

Example 7

On the contrary, if the results of the preliminary vetting procedure made by the French SA show that the Italian establishment has in fact decided to implement video surveillance system in its stores in more than one Member States as a matter of general policy and that implementation potentially infringes GDPR's provisions, for example due to allegedly excessive retention period of the video surveillance data, the resolution of the case is not only relating to the establishment located in France and the first criterion of Article 56.2 is not fulfilled.

23. If the first criterion in 56.2 is not fulfilled (the case is related to establishments located in several Member States), the SA should verify whether the second condition of Article 56.2 is satisfied, i.e. if the case's subject **matter substantially affects data subjects only in its Member State**. This is required because the two conditions of Article 56.2 are alternative (see the 'or' used to link the two conditions). The SA could also follow this second step even when there is no controller's or processor's establishment in its Member State, as its analysis will be useful for the LSA's handling of the case.

2.1.2.2 The subject matter of the complaint or the infringement substantially affects data subjects only in its Member State

¹⁰ See in particular Recital 22 of the GDPR, *Google Spain SL and Google Inc. v AEPD, Mario Costeja González* (C-131/12), and the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

¹¹ See the opinion 4/2007 of the WP29 on the concept of personal data, adopted on 20th June 2007, p. 9-12: as explained in that opinion, *mutatis mutandis*, the relationship between the case's subject matter and the controller or processor's establishment may be "*a content element or a purpose element or a result element*".

- 24. To determine whether the case has only local impacts according to the second criterion of Article 56.2 of the GDPR, the SA must determine if its subject matter substantially affects data subjects and if so, if such impact is produced only on data subjects in the SA's Member State. The SA will take into account the following precisions on a case by case basis.
- 25. The terms “*substantially affects*” have been defined in the Guidelines for identifying a controller or processor’s lead supervisory authority (WP244)¹² which have explained how the impact can be “*substantial*”¹³.
- 26. After its preliminary vetting, the SA should be in a position to consider that an actual impact is caused on data subjects. For example, it could be damaging information about the complainant disclosed on a website, a loan that was not granted because of incomplete or incorrect information, a career opportunity was thwarted because of data loss.
- 27. To be considered as a local case, the actual impact of it should be limited to data subjects residing in the SA’s Member State. On the contrary, if the SA considers that the case is likely to impact individuals in another Member State, it should consider that this is not a local case.

Example 8

A German company established in several Member States, among which Portugal, has developed an application exclusively offered to customers in Portugal. If the Portuguese SA receives a complaint against this processing or investigates a possible infringement, it may handle the case, subject to the LSA’s decision, as its subject matter impacts only data subjects in the SA’s Member State.

Example 9

An online retail company sells products that can be delivered in several Member States. The website provides information about the processing of personal data in many languages used in the European Economic Area. One linguistic version appears to be incomplete and this language is spoken only in the single Member State of the supervisory authority that receives the complaint. In this situation, the case could be considered as having only local impacts in the SA’s territory.

Example 10

On the contrary, a complaint lodged to denounce that the online order form of this retail company requires that all customers (located in several Member States) provide information that is not necessary to deliver the products¹⁴, cannot be considered as having only local impacts and must be handled by the LSA. Indeed, the subject matter of the case as well as the resolution of this case will substantially affect data subjects in other Member States and not only in the SA’s Member State.

¹² See the Guidelines for identifying a controller or processor’s lead supervisory authority, page 3: “*The most relevant ordinary English meanings of “substantial” include: “of ample or considerable amount or size; sizeable, fairly large” or “having solid worth or value, or real significance; solid; weighty, important (Oxford English Dictionary).*

The most relevant meaning of the verb ‘affect’ is ‘to influence’ or ‘to make a material impression on’. The related noun-‘effect’-means, amongst other things, ‘a result’ or ‘a consequence’ (Oxford English Dictionary). This suggests that for data processing to affect someone it must have some form of impact on them’.

¹³ See the Guidelines for identifying a controller or processor’s lead supervisory authority, p. 4: notably “*damage, loss or distress to individuals”; “limiting rights or denying an opportunity”; “affects individuals’ financial or economic status or circumstances”; “discrimination or unfair treatment”.*

¹⁴ The controller is accused to process personal data that are not “*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*” (Article 5.1(c) of the Regulation).

- 28.** A complaint about the exercise of an individual's right may reveal that it does not only affect the complainant, depending on the information that the SA has been able to gather thanks to its preliminary vetting.

Example 11

A data subject lodges a complaint because he unsuccessfully exercised his right to erasure or his right to access to a social media provider whose service is used by individuals in several Member States.

If the SA receiving the complaint can establish through publicly information, in the vetting phase, or also by way of exchanges with the competent LSA (which can be aware of a multitude of similar situation for example), that the failure to reply was contrary to the general policy of the social media provider (for example because it finds in this specific case that the complainant was requested unnecessarily to provide his/her ID contrary to the policy set out by the social media provider on its website), this complaint can be considered as having only local impacts. Conversely, when the controller's malpractice or behavior appears to be based on a general policy, the case at issue cannot be considered to have only local impact.¹⁵

2.1.2.3 The case is about an infringement of only national legislation

- 29.** Among the examples of local cases quoted by Recital 131, there is the situation where "*the processing has to be assessed taking into account relevant legal obligations under Member State law*". This could be the case where a Member State triggers exemptions or derogations provided by the GDPR or adopts a specific law that is not contrary to the GDPR.
- 30.** In other words, if a case is about a cross-border processing that is in line with the GDPR but that may infringe the national legislation of the SA's Member State, it might be an indication that the case could be considered as having only local impacts according to both Article 56.2 criteria.
- 31.** Indeed, in this situation, the subject matter of the case highly is likely to relate only to one establishment in the Member State of the SA and concerns only data subjects in that territory.

Example 12

In example 7 (the Italian main establishment of a company deciding to implement video-surveillance in each of its establishments), if the French national law about video-surveillance in public space provides that the images should not be stored more than one month, and the retention period of data is excessive only according to this national law, the resolution of the case would be only relating to the local establishment and would concern only data subjects in France. Then, the complaint could be considered as a local case according to article 56.2.

2.2 Informing the lead supervisory authority

- 32.** According to Article 56.3 "*the supervisory authority shall inform the lead supervisory authority without delay on that matter*" about the reception of the "local case" concerning a cross-border processing.

¹⁵ For a case to be considered as local, it must first be established that the impact is limited to data subjects residing in only one particular Member State or relates only to an establishment in that Member State (see paragraph 27).

- 33. Thus, as soon as the supervisory authority where the complaint was first lodged has identified that the case falls under the scope of Article 56.2, it has to inform the LSA, except when it has to reject the case which does not lie within its competence regarding the nature of the complaint¹⁶.
- 34. Once, the LSA has been identified¹⁷ (by using the information provided by the complainant, by contacting the controller or processor, or by requesting information from another SA), the receiving supervisory authority shall put the case into IMI.
- 35. If further investigations of the SA reveal that the case does not have only local impacts as it seemed to be when the SA received it and after the preliminary vetting procedure, the SA shall use the appropriate IMI procedure to transfer the case to the LSA which will handle it according to Article 56.1.
- 36. When the supervisory authority where the complaint was first lodged informs the LSA, it also explains why it considers that the case falls under the scope of Article 56.2 and why it would like to handle the case or would consider that the LSA should handle it.

2.3 Decision of the lead supervisory authority under Article 56.3

- 37. According to Article 56.3, once informed of the existence of a case with only local impacts, the LSA *"shall decide whether or not it will handle the case"*.
- 2.3.1 How does the LSA choose to handle the case or not?
- 38. As a first step, the lead supervisory authority should verify if the case falls under the scope of Article 56.2, based on the available information and on additional information the LSA may gather directly from the controller.
- 39. If the LSA considers that the case does not have only local impacts (i.e. depending on the specific configuration, its subject matter relates to more than one establishment in more than one Member State or affects data subjects in more than one Member State), it should handle the case.
- 40. If the LSA confirms that the case is a local one, it has to decide, as a second step, whether it will handle the case or let the supervisory authority where the complaint was the first lodged.
- 41. To do so, the LSA should, at least, verify two criteria:

- | The presence of an establishment of the controller or processor in the Member State of the receiving supervisory authority ;
- | Whether the case raises or not a new matter of principle which has not yet been solved at the European level.

2.3.1.1 *The presence of an establishment of the controller or processor in the supervisory authority's Member State*

¹⁶ See point 15 of the Internal EDPB Document 06/2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints.

¹⁷ See the Guidelines for identifying a controller or processor's lead supervisory authority.

- 42. Pursuant to Article 56.3, the LSA has to take “into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it”.
- 43. Recital 127 of the GDPR presents the same criterion, stating that “*when deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor*”.
- 44. Since it is the only explicitly mentioned criterion in the GDPR, the presence of an establishment under the jurisdiction of the supervisory authority where the complaint was first lodged should be a decisive aspect in the decision. Achieving an effective remedy for the data subject is the first element of ensuring a consistent and high level of protection which the GDPR intends to achieve.
- 45. Indeed, the presence of such establishment is important, in order to ensure the access to the evidence during the investigative phase and the enforceability of the final decision.
- 46. Thus, the LSA must decide to handle the case if there is no establishment in the Member State of the supervisory authority which informs it.
- 47. On the contrary, the LSA could let the supervisory authority handle the case if there is an establishment in its Member State – and if the second criterion is also fulfilled (i.e. the case does not raise a new matter of principle; see point 2.3.1.2 below).
- 48. In the situation where the LSA decides not to handle the case even if there is no controller or processor’s establishment on the territory of the receiving SA, the latter should try to informally communicate with the LSA and reach an agreement¹⁸.
- 49. If this proves unsuccessful, the SA may launch a Mutual Assistance procedure in IMI in order to request the LSA to review its position in the light of the present internal guidance. As a last resort, if the LSA still does not answer the formal request within one month¹⁹, the supervisory authority which informed it may trigger Article 64.2 with a view to obtaining an opinion from the EDPB where the LSA “*does not comply with the obligations for mutual assistance with Article 61*”.

2.3.1.2 Whether the case raises a new matter of principle

- 50. In order to ensure the consistent application of the GDPR throughout the European Economic Area, the LSA should also verify if the case raises a new matter of principle that has not yet been addressed at the European level.
- 51. A “new matter of principle” could be identified, for example where the case raises a need to interpret a specific provision that has not yet been interpreted.

Example 13

A complaint calling for an interpretation of the application of the right to restriction of processing (Article 18 of the GDPR) or a complaint raising new questions regarding the application of the right to data portability (Article 20 of the GDPR).

¹⁸ Nevertheless, this situation should be rare since it is not in line with the present internal guidance.

¹⁹ Article 61.2 of the GDPR: “*Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request*”.

- 52. By “addressed at European level” it is meant that the question raised has already been decided on the merits, either by the lead supervisory authority following the cooperation procedure, or by the European Data Protection Board (EDPB) or by the case law of the CJEU or the ECHR, while still noting that the facts of each case should be considered on their own merits.
- 53. Thus, the LSA may decide to handle a case, which could fall under the derogation of Art 56(2) GDPR if it raises a new matter of principle which has not yet been solved at the European level, even if there is a controller or processor’s establishment in the supervisory authority’s Member State.
- 54. On the contrary, the LSA could decide not to handle a local case if it does not raise a new matter of principle which has not yet been solved at the European level and if there is an establishment of the controller or processor in the Member State of the receiving supervisory authority.

2.3.1.3 Other criterion

- 55. In any case, and even if there is an establishment in the Member State of the supervisory authority and if the case does not raise a new matter of principle, the LSA still may decide to handle a local case for any other objective reason.
- 56. The LSA may decide to handle the case because it has already received several complaints against the same controller or because it would like to group several cases about a similar subject.

2.3.2 The LSA informs the supervisory authority of its decision to handle the case or not

- 57. Once the LSA has decided whether or not it will handle the case with only local impacts, and within a maximum three weeks period, it should inform the supervisory authority which received the case.
- 58. Article 56.3 of the GDPR does not specify whether the LSA has to justify its decision to handle the local case or not²⁰.
- 59. Nevertheless, the spirit and intentions of the GDPR are clearly in favour of transparency and exchange of information between supervisory authorities.
- 60. Therefore, as a good practice, the LSA should give to the supervisory authority a brief explanation of its decision, using the same dedicated form as the one used by the supervisory authority to inform the LSA of the local case.
- 61. This justification could be, for example that the LSA does not consider that the case has only local impacts and the reasons why (e.g. because it impacts data subjects in several Member States or is related to establishments located in more than one EEA territory), or that there is no processor’s or controller’s establishment in the SA’s Member State, or the LSA considers the case raises a “new matter of principle”, or any other relevant reason.
- 62. In the situation where the LSA decides not to handle the case even if there is no controller or processor’s establishment on the territory of the receiving SA, the latter should try to informally communicate with the LSA and reach an agreement²¹.

²⁰ For example, Article 57.1(g): each supervisory authority shall “cooperate with, including sharing information and provide mutual assistance to other supervisory authorities”.

²¹ Nevertheless, this situation should be rare since it is not in line with the present internal guidance.

2.3.3 What can be done when the LSA has not informed the supervisory authority of its choice during the period of three weeks?

63. As previously mentioned, according to Article 56.3 of the GDPR, the lead supervisory authority has “*a period of three weeks after being informed*” to “*decide whether or not it will handle the case*”.
64. Since Article 56.3 does not refer to the principle of “silent assent” (as, for example, Article 64.3 does), the LSA should explicitly inform the SA of its decision whether or not it will handle a case with only local impacts within this time frame. Thus, the decision to handle the case cannot be an “implied decision” or a “silent assent” of the lead supervisory authority.
65. It is possible that a supervisory authority will be met with the silence of the LSA – which, for example, did not succeed in examining the request within the allocated time.
66. In this situation, the staff of the supervisory authority shall try to contact the LSA’s staff using informal means, such as email and/or phone calls. If it is not enough to obtain an answer from the LSA, the same means could be used by the authorities’ members of the EDPB (i.e. At Commissioner or Head of Authority level²²).
67. If this informal request still proves unsuccessful, the SA may launch a Mutual Assistance procedure through the IMI system in order to request an answer from the LSA²³.
68. As a last resort, if the LSA still does not answer the formal request within one month²⁴, the supervisory authority may trigger Article 64.2 with a view to obtaining an opinion from the EDPB where the LSA “*does not comply with the obligations for mutual assistance with Article 61*”. In any case, CSAs have the possibility to trigger the urgency procedure under Article 66.

2.4 The Lead supervisory authority handles the case under Article 56.4

69. According to Article 56.4 “*where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply*”. This means that the LSA should trigger the cooperation mechanism with the other supervisory authorities concerned²⁵.
70. Doing so, “*the supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision*” (Article 56.4).
71. Since Article 56.4 provides that the supervisory authority where the complaint was first lodged “may submit” a draft decision to the LSA and Recital 127 provides that “*the supervisory authority which informed [the LSA] should have the possibility to submit a draft for a decision*”, this seems to be a discretionary choice for the supervisory authority to actually submit a draft or not.
72. Nevertheless, in some cases it could be appropriate that the supervisory authority where the complaint was first lodged submits such a draft decision to the LSA insofar as it has sufficient information at its

22 According to Article 53 of the GDPR.

23 Article 61.1 of the GDPR: “*Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner and shall put in place measures for effective cooperation with on another*”.

24 Article 61.2 of the GDPR: “*Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request*”.

25 See the Guidelines about Article 60 and the cooperation mechanism.

disposal to propose such a decision. In such cases the supervisory authority where the complaint was first lodged should inform the LSA about its intention to submit a draft decision prior to its submission.

73. The LSA shall take utmost account of the draft decision transmitted by the SA, except where there are specific, overriding reasons preventing it²⁶.
74. Indeed, Article 56.4 states that “*the lead supervisory authority shall take **utmost** account of that draft when preparing the draft decision referred to in Article 60(3)*”.
75. Recital 130 mentions on this point that “*the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged*”.
76. According to Article 60.7, when the case is resolved, the LSA should inform the supervisory authority where the case was first lodged about its final decision.

2.5 The receiving supervisory authority handles the case under Article 56.5

- 2.5.1 The supervisory authority is competent to handle the case and use cooperation measures
77. When the LSA decides not to handle the case, Article 56.6 and the Article 60 procedure do not apply for this case. In other words when the cross-border case is handled “locally”, the LSA is not the sole interlocutor of the controller or processor.
78. Indeed, Article 56.6 is a general rule applying when the LSA handles the case. It does not apply when the case is handled under Article 56.2 in conjunction with Article 56.5 that lay down a derogation (the case with local impacts is handled by the local supervisory authority where the complaint was first lodged or which first detects a possible infringement).
79. The supervisory authority shall exercise its full range of powers pursuant to Article 58, including the corrective powers. The SA is then the only competent authority for this case.
80. According to Recital 131, however it is suggested, as a good practice, that the receiving supervisory authority which is dealing with a case contacts the controller and the processor, through its establishment present in its Member State, in order to “*seek an amicable settlement with*” it²⁷.
81. According to Article 56.5, “*where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to articles 61 and 62*”.
82. Article 61 provides the use of mutual assistance which covers, in particular, “*information requests and supervisory measures, such as requests to carry out prior authorizations and consultations, inspections and investigations*”.

26 See the Guidelines about Article 60 and the cooperation mechanism.

27 Depending on the national procedural legislation.

- 83. Articles 62 provides the conduct of joint operations “*including joint investigations and joint enforcement measures*”.
- 84. Articles 61 and 62 provide different degrees of mutual assistance and joint operations that should be triggered depending on the circumstances of the case at stake. Consequently, the supervisory authority should use one or both of these two mechanisms, when it finds it necessary in the process of handling a case with only local impacts.
- 85. For example, the mutual assistance may consist for the supervisory authority to request information from another supervisory authority which also has a controller’s establishment in its Member State.
- 86. Joint operations may be appropriate, for example, if an investigation needs to be done in the premises of a processor located in a Member State other than that of the controller or processor involved in the local case at hand.
- 87. Even though in some cases it might not be necessary or effective to use either the mutual assistance or the joint operations for handling of the case the SA will, as a best practice, inform the LSA about the outcome of the local case, through the IMI system.

2.5.2 How and by whom is a binding decision imposed to the controller or the processor?

- 88. If the attempt to reach an amicable settlement with the controller or processor proves unsuccessful, the supervisory authority receiving a complaint or detecting an infringement “*exercises its full range of powers*” (Recital 131).
- 89. According to Article 55.1, “*Each supervisory authority shall be competent for the performance of the tasks assigned to and then exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*”.
- 90. Moreover, Recital 122 adds that “*this should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation*”.
- 91. These provisions lay down the principle of the competence of a supervisory authority on the territory of its own Member State. Conversely, a supervisory authority is not competent on the territory of another supervisory authority’s Member State.
- 92. Thus, where the SA decides to adopt corrective measures pursuant to the GDPR’s provisions or its national law, the binding decision should be imposed to the controller or processor’s establishment in its own Member State. If that establishment happens to be the main establishment in the EU, i.e. if the SA is the LSA, those measures will be applied by the controller in all its establishments and thus produce effects in other MS as well.

2.6 Informing the complainant

93. According to Articles 60.7²⁸ and 77.2²⁹ of the GDPR, whether the case with only local impacts is handled by the LSA or by the supervisory authority where the complaint was first lodged, this latter remains the sole interlocutor of the complainant.
94. The lead supervisory authority which handles the case shall inform the supervisory authority where the complaint was first lodged of the decision it has made in this case (corrective measures imposed to the controller/processor, amicable settlement reached with the controller/processor, etc.). The SA will then inform the complainant about this decision.

2.7 Handling a case by the lead supervisory authority under Article 56.2

95. Article 56.1 provides that “the supervisory authority of the main establishment or of the controller or processor shall be competent to act as a lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60”.
96. Thus, as a principle the LSA is competent to handle a case about a cross-border processing carried out by a controller or processor which has its main or its only establishment in its Member State.
97. As explained above, Article 56.2 lays down a derogation to this principle when the case has only local impacts: the authority receiving a complaint or informed of an infringement may be competent if the case has only local impacts in its Member State.
98. A supervisory authority which is the LSA with respect to a particular cross-border processing may receive complaints which have only local impacts in its own Member State. If, after careful consideration of the circumstances of the case, the receiving SA has been satisfied that the case is to be considered local under Article 56.2, there is no need to contact other supervisory authorities. This implies that other authorities are not involved in the proceedings.
99. When considering the involvement of other supervisory authorities, careful attention must be given to the procedure as provided for by the GDPR. Compliance with procedural rules may be subject of judicial review in case the decision is challenged before the court. The lead authority should attempt to trace the authorities concerned, thus ensuring the correct application of the procedural rules.
100. When the LSA handles a local case as a supervisory authority which received the complaint in question, it acts in accordance with the procedure described in the part 2.5.

For the European Data Protection Board

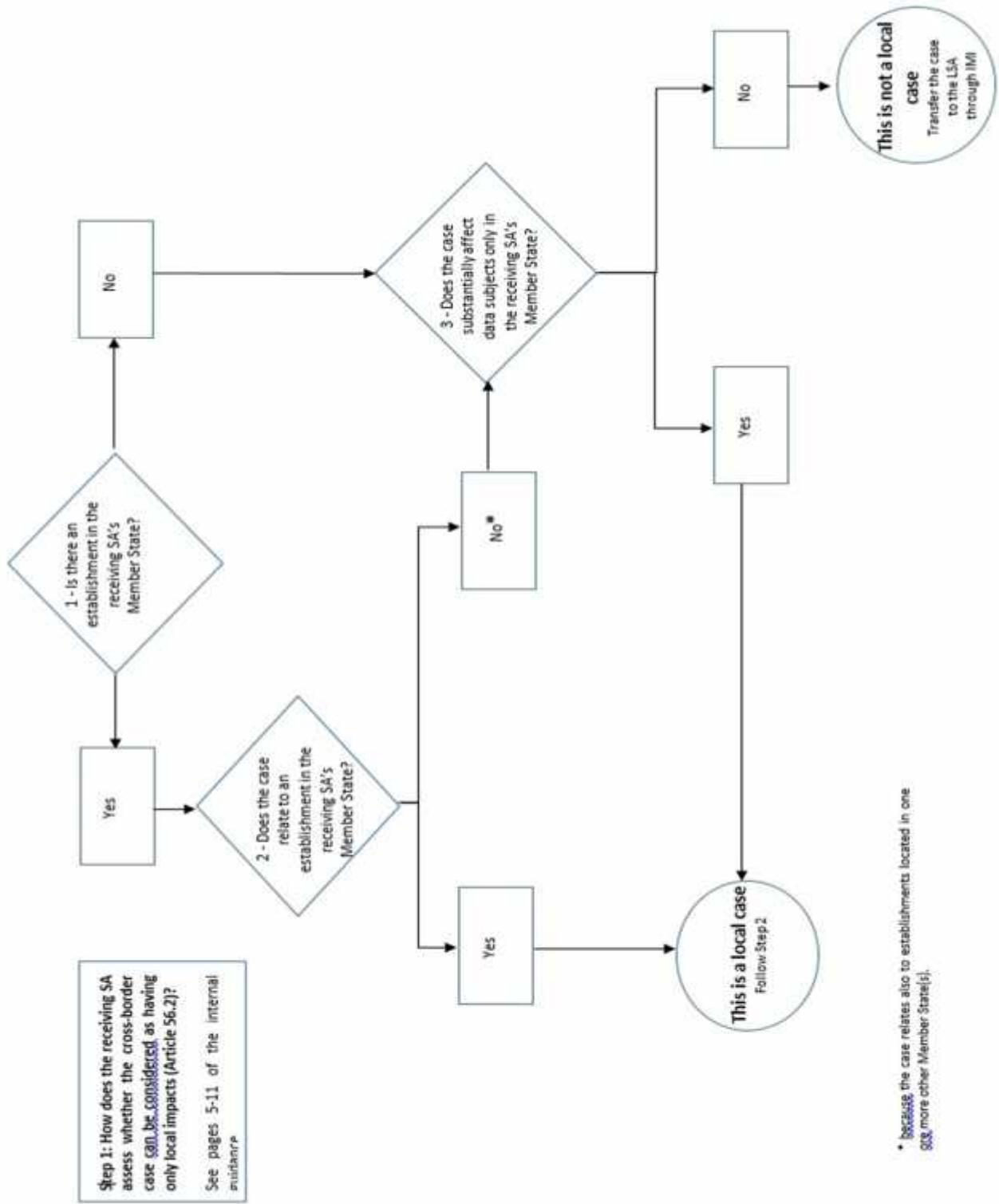
The Chair

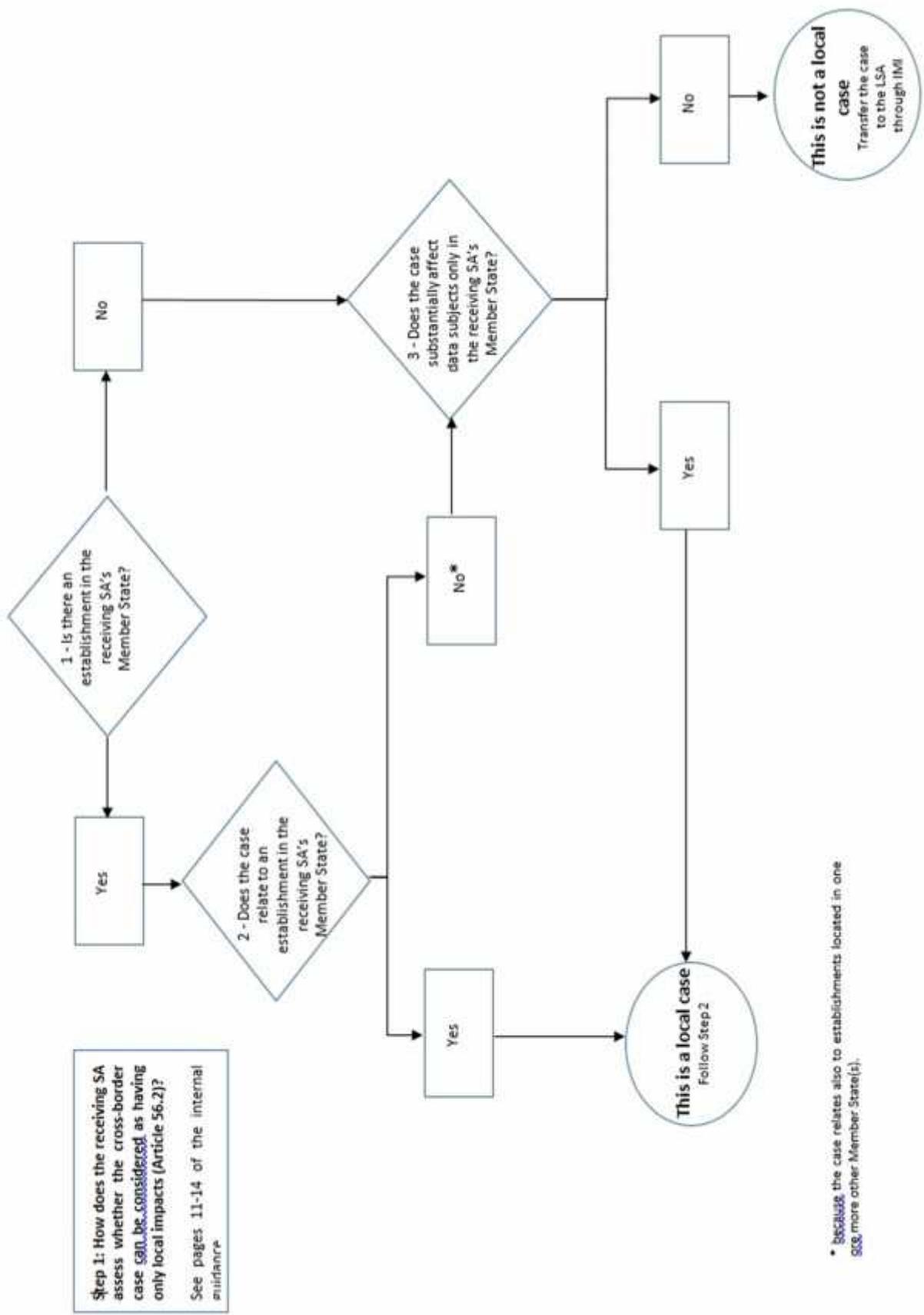
(Andrea Jelinek)

28 Article 60.7: “The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision”.

29 Article 77.2: “The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint”.

ANNEX: FLOWCHART





Internal EDPB Documents



Internal EDPB Document 2/2019 on Proposals for Common Strategic Priorities for Supervision and Guidance

Adopted on 4 June 2019

IMPORTANT NOTE:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website. This document contains proposals from one of the EDPB Expert subgroup in relation of the Coordinated Enforcement Framework (CEF). In the meantime, the EDPB adopted a document dedicated to this CEF and decided on the CEF topic for 2022. Therefore, some of the information in this document may no longer be up to date.

This document contains redactions as the publication of this information would undermine the commercial interests of a natural or legal person.

Table of contents

1	Introduction.....	3
2	Proposals for common strategic priorities.....	4
2.1	Adtech	4
2.2	Third Party Apps/APIs.....	5
2.3	Data Brokers.....	6
2.4	Data subject's right to object to direct marketing (Art. 21(3) GDPR)	7
2.5	Processing of personal data of non-members of social networking services	9
2.5.1	General risks regarding the processing of personal data of "non-members"	9
2.5.2	Standard of protection for "non-members"	9
2.5.3	Third party apps as multipliers.....	10
2.5.4	Unlawfulness of the processing and supervision of joint controllers	10
2.6	Interplay between the ePrivacy Directive and the GDPR.....	11

The European Data Protection Board

Having regard to Article 70 (1) (e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

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

Having regard to Article 3 and Article 22 of its Rules of Procedure as amended on 23 November 2018,

HAS ADOPTED THE FOLLOWING INTERNAL DOCUMENT

1 INTRODUCTION

1. One of the mandates of the Social Media Expert Subgroup (hereinafter “SOCM ESG”) is to propose strategic priorities for supervision and guidance. As stated in the Workplan of the SOCM ESG, while providers of social media may have a lead supervisory authority within the “one stop shop” GDPR mechanism, the supervision of other actors, which are associated with, related to or interlinked with social media platforms, is often the responsibility of other supervisory authorities. The SOCM ESG’s mandate also recognises that the regulation of the processing of personal data that takes place in the context of social media may be rendered more effective if supervisory authorities agree upon common strategic supervision priorities.
2. Pursuant to its mandate, the SOCM ESG has identified strategic priorities for supervision on the basis of trends in data subject complaints, technological trends, findings or milestones in national investigations concerning social media and related actors. This internal document identifying proposals for common strategic priorities for supervision and guidance is therefore complementary to and recognises the role of competent supervisory authorities (including lead supervisory authorities) in their enforcement activities under the GDPR. The SOCM ESG recognises that these strategic priorities are best tackled in conjunction with other Subgroups, in particular to ensure efficient use of resources and avoid overlap between Subgroups.
3. The present internal document identifies common strategic priorities and recommendations in relation to these priorities (i.e. the Recommendations). Most Recommendations include cooperation with between Subgroups including cooperation with the SOCM ESG. In respect of these Recommendations, it is therefore proposed that the SOCM ESG cooperates with the other Subgroups identified as the strategic priorities either within existing Workplans or in respect of a standalone work items in the future.
4. Where issues are proposed for consideration by other Subgroups, it is recognised that it is entirely a matter for each Subgroup how it wishes to address the relevant issue. For example, where issues have been referred to the Enforcement Expert Subgroup (hereinafter “ENF ESG”), it may be that this issue may form part of the coordinated enforcement framework (hereinafter “CEF”), which is currently under consideration in that context.

2 PROPOSALS FOR COMMON STRATEGIC PRIORITIES

5. The following strategic priorities have been identified by the SOCM ESG:
 - a. Adtech
 - b. Third-party Apps/APIs
 - c. Data brokers
 - d. Data subject's right to object to direct marketing
 - e. Processing of personal data of non-members of social media services
 - f. Interplay between the ePrivacy Directive and the GDPR.
6. In respect of each strategic priority, a number of possible recommendations are identified for potential next steps (the Recommendations). While each recommendation could be beneficial, one recommendation is identified in particular in relation to each identified strategic priority (i.e. the recommendation that carried the broadest support within the SOCM ESG).

2.1 Adtech

7. The adtech sector encompasses a vast array of actors including advertisers, publishers, ad networks, ad exchanges, demand-side and supply-side platforms, data management platforms. It has emerged as a separate eco-system within the online environment which permeates all social networking services as well as extending further to almost all categories of internet activity. Some of the key questions which arise in relation to the regulation of the adtech sector from a data protection law perspective are:
 - a. Data subjects' perceived loss of control of their personal data once collected and its consequences including the exercise of data subject rights;
 - b. Lawful bases of personal data processing in the context of the adtech industry;
 - c. Further processing of personal data collected for specific purposes;
 - d. Processing of special categories of personal data;
 - e. Employment of data protection by design and default; and
 - f. Standard of technical and organisation measures employed in relation to personal data processed in the adtech ecosystem.
8. When considering this topic, the [REDACTED] Framework should also be considered, as it is one to which many in the adtech sector align themselves.

9. Recommendation 1

It is recommended that the [REDACTED] industry bodies/ appropriate parties are engaged with via an EDPB stakeholder group with the aim of increasing compliance and reducing complaints. It is recommended that the EDPB stakeholder group could include members from the SOCM ESG, the Technology Expert Subgroup (hereinafter “TECH ESG”), the ENF ESG and the Compliance, e-Government and Health Expert Subgroup. This paper and therefore this recommendation of participation in a potential EDPB Adtech stakeholder group has been mentioned at recent meetings of the aforementioned Subgroups.

10. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 1 may be:
 - a. Develop (additional) guidance: the TECH ESG might develop further guidance addressing this issue, for example by:
 - i. Updating Opinion 2/2010 on online behavioural advertising;¹
 - ii. Updating Opinion 2/2013 on obtaining consent for cookies;²
 - iii. Assessing and/or reviewing the [REDACTED] Framework.
 - b. The ENF ESG could also consider this issue further as part of the CEF.

2.2 Third Party Apps/APIs

11. Many major online platforms, including (but not limited to) social networks such as [REDACTED] [REDACTED], enable third parties to develop apps on those platforms which can process users' personal data. The third parties involved may include actors within the online advertising sector as mentioned under “Adtech”. Compliance with data protection law by online platforms and third party app developers requires fresh scrutiny under the GDPR, due to the potential risks to individuals in terms of transparency, lawful basis, consent and other key data protection principles such as purpose limitation, data minimisation and security of processing. Third-party apps/APIs are also broader in scope than the facilities major social media platforms offer developers, encompassing much of the online and particularly the mobile eco-systems. Given the state of the art of technological development and the ways in which users currently interact with online services, we believe there are clear risks posed to individuals and that SAs should ensure that actors in this space are appropriately complying with data protection obligations.

¹ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

² https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

12. Recommendation 2

It is recommended that this issue be further developed as part of SOCM ESG's Work Item 3 "Governance of social media platforms", which is planned for later in 2019. SOCM ESG also proposes to engage with the ENF ESG (e.g. in order identify case studies), the TECH ESG (e.g. regarding measures to limit misuse) and Key Provisions Expert Subgroup (e.g. as regards possible arrangements among controllers), as appropriate.

13. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 2 may be:

- a. Develop (additional) guidance: the TECH ESG or Key Provisions Expert Subgroup (hereinafter "KEYPRO ESG") might also further address this matter, for example by:
 - i. Updating Opinion 5/2009 on online social networking;³ and/or
 - ii. Updating Opinion 02/2013 on apps on smart devices.⁴
- b. The ENF ESG could also consider this issue further as part of the CEF.

2.3 Data Brokers

14. Data brokers collect personal data and resell or share that information with other stakeholders. In other words, they aggregate data collected from a wide variety of sources. They subsequently transfer the aggregated data to third parties, i.e. their clients, for a variety of purposes, including targeting of data subject (advertisement, improvement of customer experience), and fight against fraud for example.
15. Generally speaking, there are two situations: in the first one, the data broker acts as an intermediary between its clients who are seeking to monetise their databases on the one hand, and those that are seeking to enrich their databases on the other. Here, the broker acts on behalf of and in the name of its clients. In the second case, the data broker centralises, aggregates and enriches the data on his own account, and sells this enriched data to other stakeholders.
16. Sources of personal data might include the following: (i) database formed as part of the relationship between a company and its customers (classic customer files, loyalty programs, etc.), (ii) data derived from the data subject's navigation activity (cookies, fingerprint and other tracers), (iii) the use of mobile applications, and (iv) the data relating to purchases made online.
17. There are many issues that have been identified regarding this type of processing, of which transparency is one. Indeed, it is common practice for data controllers to collect the consent for the transmission of the personal data by simply including the "partners", without even providing information on the purpose of the processing or the identity of the recipients. In addition, certain data brokers may not inform data subjects on their role as data controllers or

³ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

⁴ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

on their rights. In this sense, the EDPB should provide guidelines on the precise information that data brokers need to provide to data subjects and possible best practices for doing so.⁵

18. Another issue which should be tackled by the EDPB is one of the legal basis. First of all, when the legal basis is consent (for instance because the processing involves the implementation of a tracking device for advertisement purposes), it may be that the clients of the data brokers have no way of proving that the data subject has consented to the re-use of their data by the data brokers and their transmission to them. In addition, the lack of specificity of consent due to the above-mentioned lack of transparency, may deprive the partners' processing of a legal basis, which would render the re-use of the data purchased from the data broker unlawful. Furthermore, it appears that many data brokers seek to rely on legitimate interests for their processing. It is proposed that the EDPB provide practical examples and concrete guidelines on the circumstances in which legitimate interest would be a valid legal basis. Indeed, the opacity of the online advertising industry, the difficulty for the data subject to identify the data controllers processing their data, and the lack of true control that they may exercise (including the ability to exercise the unconditional right to opt-out of direct marketing (article 21 (2)), may mean that legitimate interest may not be employed as a lawful basis for the relevant processing.

19. Recommendation 3

It is recommended that the ENF ESG could consider this issue in the context of the CEF.

20. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 3 may be:
- a. Develop (additional) guidance: Subgroups such as the TECH ESG or KEYPRO ESG could further progress this issue (e.g. in the context of the update of the opinion on legitimate interest and/or future work items of the TECH ESG).
 - b. The SOCM ESG could also refer to the role of data brokers in the context of SOCM ESG's Work Item 1 and/or 3.

[2.4 Data subject's right to object to direct marketing \(Art. 21\(3\) GDPR\)](#)

21. Articles 21(2) of the GDPR provides that where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Article 21 (3) also states that where the data subject objects to processing for direct marketing purposes, the personal data shall no longer

⁵ It is indeed important to remind data brokers that article 14 of the GDPR requires that they inform the data subject within a month before starting processing the data on their own account. It may also be necessary to remind data controllers that as stated in article 13 of the GDPR, they need to inform the data subject before transmitting the data to data brokers. In this sense, the EDPB could recommend concrete solutions, such as presenting the data subject with the boxes: one for consenting to the collection of the data processed and the profiling by the data controller, and the second one for the processing to be carried out by partners, including data brokers. A hyperlink could also be provided with an updated listing the names of data brokers who are the recipients as well as data controllers of the data.

be processed for such purposes. Article 21(5) provides that in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

22. It appears that the right to object is absolute and that once the data subject has exercised this right, the controller needs to stop the processing of personal data for direct marketing purposes. There are however a few questions relating the right of objection for direct marketing purposes which would benefit from a harmonised approach at the European level.
23. First of all, the concept of “direct marketing” is not clearly defined in the GDPR and may, in some situations, be difficult to delineate precisely. For instance, in the context of social media, the scope of the definition of “direct marketing” may be a little difficult to identify. Indeed, some social media providers offer advertisers tools (such as the use of “Lookalike Audiences” by Facebook) which enable an advertiser to target people who are similar to their existing customers. In this situation, it is not clear whether the existing customers are being “directly marketed” to or not, as they are not receiving any targeted advertisement themselves but at the same time, their personal data is being processed for the purposes of targeting other data subjects. Speaking more broadly, it should be clarified whether or not targeted display ads are included within the scope of direct marketing. It would be beneficial to all stakeholders to clearly determine the scope of direct marketing, insofar as the GDPR does not provide a clear definition of this concept.
24. Secondly, the GDPR is not clear whether the controller needs to delete the data as well once the data subject objects to the processing for direct marketing purposes. One might consider that the controller only needs to stop the processing of the data for this purpose and to ensure that their preference not to receive direct marketing solicitations is complied with. This is a question which could be addressed at European level.
25. Another point which should be addressed at the European level is the question of tracking techniques, including cookie-based technologies, social plugins and tracking pixels that are stored on the terminal equipment of the data subject. The EDPB is aware of the review of the ePrivacy Directive (2002/58/EC), which requires the collection of consent for most online marketing messages or marketing calls, and online tracking methods including the use of cookies or apps or other software. Indeed, article 5(3) of the ePrivacy Directive requires prior informed consent for storage or for access to information stored on a user's terminal equipment. The EDPB could also clarify that in addition to the right of objection which is absolute for the processing for direct marketing purposes, the data subject should be able to withdraw his or her consent as easily and without any justification. The EDPB could also recall that in respect of personal data which the right to erasure is exercised in accordance with article 17(1)(b) GDPR, the controller is obliged to erase such personal data “without undue delay”.
26. Furthermore, the EDPB could clarify when the right to object to the processing for direct marketing under article 21 of the GDPR is exercisable in respect of direct marketing. It is worth noting that according to article 21, the data subject can object to the processing at any time. Some Member States even consider that the right to object can be exercised before the processing takes place. A harmonized approach on this point is also recommended at the European level.
27. Finally, processing of personal data for marketing purposes often involves a significant number of stakeholders (partners, data brokers, data processors...), who may, under article 26 of the

GDPR, be categorised as joint controllers. Data subjects should be able to exercise their right of objection to any of the data controller who must then put in place processes to reflect the will of the data subject to the next “link” in the chain.

28. Recommendation 4

It is recommended that SOCM ESG could provide assistance to KEYPRO ESG in the development of guidance on this issue, specifically in the context in the proposed guidance in respect of data subject rights, which is scheduled for 2019.

29. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 4 may be:

- a. SOCM ESG could also consider dealing with this issue as part of SOCM ESG’s Work Item 1 or 3;
- b. ENF ESG could also consider this issue further as part of the CEF.

2.5 Processing of personal data of non-members of social networking services

30. Certain social media providers also process the personal data of people who are not members of the social networking service, for example, by tracking their browsing behaviour across multiple websites or by collecting such information through mobile applications. Collection of personal data of non-members may be achieved using technical tools (such as cookies) and browser information and other tools developed by social media providers. In this context, the existence of a legal basis for the processing of non-member personal data should be examined.

2.5.1 General risks regarding the processing of personal data of “non-members”

31. The general risk of the processing of personal data of social media users is already being addressed by the SOCM ESG in the context of Work item 1 (the targeting of social media users) which identifies inter alia the following risks: risks related to privacy and protection of personal data, discrimination, manipulation, the interference of political discourse and democratic electoral process and chilling effects on freedom of expression and the restraint of access to information.

32. In regard to “non-members” these risks are increased by a lack of transparency. The reasonable expectations of the individual without a specific social media account do not include the systematic targeting and profiling of their person.

2.5.2 Standard of protection for “non-members”

33. In its decision of June 5, 2018 (file number C-210/16), the Court of Justice of the European Union ruled that a “fan page administrator’s responsibility for the processing of the personal data of (non-members) appears to be even greater, as the mere consultation of the homepage by visitors automatically starts the processing of their personal data.” This emphasises the high level of protection that is needed regarding the persons whose personal data are processed by the social networking services without having an account on the relevant platform. Because of the non-transparent practices in this field, there are a high number of data subjects who are not in a position to anticipate and assess the processing of their personal data. This

corresponds with the general risk regarding the processing of personal data of “non-members”.

2.5.3 Third party apps as multipliers

34. The described risks are usually multiplied by the use of third party apps and the combination of the data collected of the social network service and the data processed by the operators of the third party apps. Through the processing of personal data across different applications a profiling and systematic monitoring could be established. As different actors in this ecosystem of data processing in the social media and advertisement sector share the data of many individuals and evaluate and score these individuals in order to make decisions and assessments about them, these risks are also relevant for “non-members”.

2.5.4 Unlawfulness of the processing and supervision of joint controllers

35. With regard to Work Item 1 of the SOCM ESG concerning the targeting of social media users and the definition of joint controllers under Article 26 GDPR, this issue may stretch beyond controllers or processors of social media services. According to Article 26 GDPR specific operators of a fan page or other comparable types of social media accounts can be held responsible for the processing of personal data of “non-members” of these platforms. Therefore, supervisory authorities should raise the awareness of this common responsibility. The first step which could be taken are informal or formal investigations and the German Conference of the Independent Data Protection Authorities of the Federal State and the Länder (DSK) has provided an example in form of a questionnaire in its “DSK decision regarding Facebook Fan Pages”.⁶

36. Recommendation 5

It is recommended that SOCM ESG address this issue as part of SOCM ESG’s Work Item 3 “Governance of social media platforms”, which is planned for later in 2019. In this context and in developing Work item 3, the SOCM ESG plans to, at the appropriate time, seek the input from both the TECH ESG and KEYPRO ESG.

37. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 5 may be:

- a. Develop guidance: the SOCM ESG or another Subgroup (such as the TECH ESG or KEYPRO ESG) could progress this issue, for example by updating Opinion 4/2012 on Consent Exemption,⁷ 2/2010 on Online Behavioural Advertising⁸ and 5/2009 on Online Social Networking.⁹
- b. Develop additional guidance: the SOCM ESG could further progress this topic.
- c. ENF ESG could also consider this issue further as part of the CEF.

⁶ https://datenschutz-hamburg.de/assets/pdf/DSK-decision_regarding_Facebook_Fan_Pages.pdf

⁷ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

⁸ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

⁹ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

2.6 Interplay between the ePrivacy Directive and the GDPR

38. There are processing activities which trigger the material scope of both the GDPR and the ePrivacy Directive. For example, the gaining of access to information stored in an end-user's device may also give rise to the processing of personal data. If that is the case, both Article 5(3) of the ePrivacy Directive and the GDPR shall apply.¹⁰
39. The aim of the ePrivacy Directive is to particularise and complement the provisions of the GDPR.¹¹ As a "lex specialis", the ePrivacy Directive takes precedence over the (more general) provisions of the GDPR insofar as the matter is specifically addressed by the ePrivacy Directive.¹²
40. While the interaction between the ePrivacy Directive and Directive 95/46 has already been addressed in previous WP29 guidance, questions have emerged regarding the competence of supervisory authorities to exercise their powers under the GDPR in cases where both the GDPR and national implementations of the ePrivacy Directive are applicable.
41. The ePrivacy Directive allows Member States to assign supervisory competences to national regulatory authorities other than data protection authorities. It does not, however, stipulate that the supervision of its provisions shall be the exclusive competence of such a national regulatory authority,¹³ and, as stated above, this is a matter for national Member State law. The question may be asked to what extent data protection authorities should consider the provisions of the ePrivacy Directive when exercising their powers under the GDPR (e.g., when assessing the lawfulness of processing). Closely related is the question of whether the applicability of ePrivacy rules imposes any limits on the handling of cases in the context of the cooperation and consistency mechanisms of Chapter VII, and if so, to what extent. Further clarification may also be necessary regarding the extent to which a set of processing operations can be governed by provisions of the ePrivacy Directive and the GDPR (e.g. in terms of lawfulness of processing including consent, principles relating to the processing of personal data, transparency, etc).

42. Recommendation 6

No further immediate action recommended given the outcome of the Art. 64(2) GDPR opinion launched by the Belgian DPA on this topic. Additional guidance may be provided in the context of other work items, as appropriate (e.g. C-ITS).

¹⁰ See e.g. Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 9 ("*If as a result of placing and retrieving information through the cookie or similar device, the information collected can be considered personal data then, in addition to Article 5(3), Directive 95/46/EC will also apply.*").

¹¹ Article 1(2) of Directive 2002/58 as amended by Directive 2006/24/EC and Directive 2009/136/EC in light of article 94(2) of the GDPR.

¹² Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 10. See also recital (173) GDPR ("*This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council (2), including the obligations on the controller and the rights of natural persons. [...]*")

¹³ On the contrary, the ePrivacy Directive explicitly recognises that multiple authorities may be competent for its supervision and enforcement. See article 15a of Directive 2002/58 as amended by Directive 2006/24/EC and Directive 2009/136/EC.

43. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 6 may be:

- a. The ENF ESG could also consider this issue further as part of the CEF.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Internal EDPB Documents



Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements

Version 1.0

Adopted on 2 February 2021

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of contents

1	Introduction.....	3
2	Legal framework.....	4
2.1	Introduction.....	4
2.2	Legal framework.....	4
2.2.1	Article 57(1): Tasks of supervisory authorities	5
2.2.2	Article 58(1): Investigative powers of supervisory authorities	6
2.2.3	Article 77: The right to lodge a complaint with a supervisory authority	7
2.2.4	Article 78: Right to an effective judicial remedy against a supervisory authority	7
2.3	EU Case law	8
3	Investigating complaints	11
3.1	Introduction.....	11
3.1.1	The role of national procedural law	11
3.1.2	Procedural rights of the complainant under the GDPR and general principles of law	12
3.2	Definition of a complaint.....	13
3.3	“Investigate” the subject matter of the complaint	14
3.4	Investigate “to the extent appropriate”	15
3.5	Conclusion	16
4	Information related to a possible infringement of data protection law.....	16
4.1	Introduction.....	16
4.2	Legal Framework	17
4.3	Conclusion	17

The European Data Protection Board

Having regard to Article 57(1)(f) and Article 77 and Article 78 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

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

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

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 INTRODUCTION

1. During the 10th plenary meeting on the 9-10 July 2019, the EDPB granted the Enforcement Expert Subgroup a mandate to:
 - a. Develop a common interpretation of Article 57(1)(f) and a common understanding of the minimum requirements to fulfil the obligation to “investigate the complaint to the extent appropriate”,
 - b. Assess how supervisory authorities deal with information related to a possible infringement of data protection law in order to evaluate the need for developing guidelines or other tools that ensure a consistent approach, in particular in relation to the impact on the cooperation mechanism,
 - c. Assess the practice of supervisory authorities on what constitutes a draft decision pursuant to Article 60(3) and reach a common understanding about it as well as on when there is no need to create such a decision,
 - d. Assess in the case of cross-border processing, whether and in what way there is an obligation for the competent authority in the event of notification by a supervisory authority concerned of a possible infringement of data protection, to submit a draft decision in accordance with the second sentence of Article 60(3) GDPR even if there is no specific reference to a complaint within the framework of the regulation on the cooperation procedure
2. The present document concerns only question one and two of the mandate. It is in terms of its scope not limited to the handling of complaints and information related to possible infringements that are cross-border in nature. The first section of this paper aims to create a shared understanding of the obligation under 57(1)(f) in general and the second section aims to ensure a consistent approach concerning information related to a possible infringement.

2 LEGAL FRAMEWORK

2.1 Introduction

3. The fundamental right of data protection as enshrined in Article 8 of the Charter of Fundamental Rights (“The Charter”) provides *inter alia* that compliance with data protection rules shall be subject to control by an independent authority.
4. In ensuring such control, the GDPR aims at providing a more coherent data protection framework in the European Union backed by strong enforcement.
5. It is thus the task of supervisory authorities to monitor and enforce the GDPR. This is set out in Article 57 that amongst the listed supervisory duties outlines that supervisory authorities shall handle and investigate complaints from data subjects. This key duty of supervisory authorities corresponds with the right of data subjects pursuant to Article 77 to lodge a complaint with a supervisory authority. As “monitoring bodies”, supervisory authorities function as complaint handling bodies as well as being empowered to undertake independent supervisory activities necessary for the performance of their supervisory duties.
6. In order to ensure a consistent and high level of protection of natural persons, the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data should be equivalent in all Member States. Data subjects shall enjoy equal access to exercise their right to data protection regardless of which supervisory authority would handle a given complaint.
7. With a view to ensuring a consistent and homogenous level of protection, it is important that supervisory authorities share a common understanding of their tasks, including that of handling complaints from data subjects. When applying the provisions of the GDPR, the overarching purpose of ensuring a uniform level of protection of natural persons with regard to the processing of personal data must be taken into account. The enforcement of these rules should contribute to this. Moreover, an interpretation of a given provision must not undermine the effectiveness of EU law and its principle of primacy in an area that has been regulated by the EU (see below regarding the principle of procedural autonomy).

2.2 Legal framework

8. While acknowledging that the previous legal frameworks under the previous Directive 95/46 (“the Directive”)¹ have been applied in slightly different contexts, it is relevant to recall the essential predecessor provisions in order to properly assess the application of provisions of the Regulation.
9. The tasks of supervisory authorities were not comprehensively described in Directive 95/46. Article 28(1) merely stated that the authorities were responsible for monitoring the application of the provisions adopted by the Member States pursuant to the Directive. Article 28(4) referred to the task of hearing claims and the right to be informed of the outcome hereof.

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

10. On 25 January 2012, the European Commission presented its proposal for the General Data Protection Regulation² to replace Directive 95/46. One of the circumstances leading to the new legal framework was, as stated in the Commission Staff Working Paper Impact Assessment³, that individuals in practice enjoyed different data protection rights, due to fragmentation as well as inconsistent implementation and enforcement in different Member States. To this end, the proposal for a new Regulation *inter alia* focused on ensuring stronger enforcement of the rules.
11. Chapter VI (Independent supervisory authorities) of the GDPR reinforces *inter alia* the role and powers of supervisory authorities. Article 57(1) lists the tasks of supervisory authorities, whereas Article 58(1) of the GDPR lists the investigative powers that the supervisory authorities shall have. When comparing the tasks of supervisory authorities as held in Article 57 of the GDPR with the tasks of supervisory authorities under the previous legal framework, it appears that the number of tasks have been expanded or strengthened.
12. Chapter VIII (Remedies, liability and penalties) includes provisions that strengthen the legal position of data subjects *vis-a-vis* supervisory authorities in providing the data subject with a right to lodge a complaint and to an effective judicial remedy against a supervisory authority.

2.2.1 Article 57(1): Tasks of supervisory authorities

13. Article 57 enumerates several tasks of supervisory authorities.
14. Article 57(1) provides *inter alia* that:
 1. *Without prejudice to other tasks asset out under this Regulation, each supervisory authority shall on its territory:*
 - (a) *monitor and enforce the application of this Regulation;*
[...]
 - (d) *promote the awareness of controllers and processors of their obligations under this Regulation;*
[...]
 - (f) *handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;*

² Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) /* COM/2012/011 final - 2012/0011 (COD) */

³ COMMISSION STAFF WORKING PAPER Impact Assessment /* SEC/2012/0072 final *//<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0072>

- (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
- [...]
15. This Article should be read in conjunction with Recital 129, which provides that: "*In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings.*

[...]The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision."

2.2.2 Article 58(1): Investigative powers of supervisory authorities

16. In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority.

Article 58(1) provides that:

Each supervisory authority shall have all of the following investigative powers:

- (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;*
- (b) to carry out investigations in the form of data protection audits;*
- (c) to carry out a review on certifications issued pursuant to Article 42(7);*
- (d) to notify the controller or the processor of an alleged infringement of this Regulation;*
- (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;*

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2.2.3 Article 77: The right to lodge a complaint with a supervisory authority

17. Article 77 stipulates the right of data subjects to file a complaint with a supervisory authority regarding an alleged infringement of his or her personal data. The provision also sets out a duty to inform the complainant on the progress and outcome of the complaint.
18. Article 77 provides that:
 1. *Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*
 2. *The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.*

19. In the context of the right to lodge a complaint should be read in conjunction with Recital 141: “*Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject.*

The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject [...].

2.2.4 Article 78: Right to an effective judicial remedy against a supervisory authority

20. Article 78 sets out the right to an effective judicial remedy against a legally binding decision of a supervisory authority and against an ‘inactive’ supervisory authority.

Article 78 provides that:

1. *Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.*
2. *Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.*
3. *Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.*

4. *Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.*
21. This Article should be read in conjunction with Recital 143, which provides that:
- "Each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority."*
- ### 2.3 EU Case law
22. The importance of consistent and homogeneous EU data protection rules - in particular as regards the independency and the powers of the supervisory authorities in light of Article 8(3) of the Charter and Article 16 TFEU - has been underlined by the Court of Justice of the European Union ("Court of Justice" or "the Court"). The Court of Justice has consistently emphasized that control by an independent authority is an essential component of the right to protection of personal data.
23. In its judgment of 6 October 2015, *Schrems* (C 362/14, EU:C:2015:650), the Court underlines that "*As regards the powers available to the national supervisory authorities (...) Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU. In order to guarantee that protection [of individuals with regard to the processing of personal data], the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data. The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.*"⁴
24. Moreover, the Court noted – in the context of a Commission decision pursuant to Article 25(6) of Directive 95/46 – that it is incumbent upon a supervisory authority to examine the claim from the data subject regarding the protection of his or her privacy with “all due diligence”: “*Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings,*

⁴ Para. 40, 42 and 43.

the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence”⁵.

25. The Court stressed in its judgement of 16 July 2020, Facebook Ireland and Schrems (Case C-311/18, EU:C:2020:559) that the primary responsibility of supervisory authorities is to monitor the application of the GDPR and to ensure its enforcement: “*In accordance with Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data.[....]⁶. It follows from those provisions that the supervisory authorities’ primary responsibility is to monitor the application of the GDPR and to ensure its enforcement. [....]*⁷”.
26. Furthermore, the Court underlined with reference to Article 57(1)(f) and Article 77(1) that supervisory authorities must handle a complaint with all due diligence and examine the nature of the complaint as necessary: “*In addition, under Article 57(1)(f) of the GDPR, each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that data subject considers that the processing of his or her personal data infringes the regulation, and is required to examine the nature of that complaint as necessary. The supervisory authority must handle such a complaint with all due diligence (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C 362/14, EU:C:2015:650, paragraph 63)*⁸”.
27. As to the means of investigation and its outcome the Court highlights the supervisory authority’s investigative powers in Article 58(1) and its corrective powers in Article 58(2) GDPR: “*In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt.*⁹ Even though the judgment of the Court references actions related to unlawful transfer of personal data to third countries, the EDPB recognizes that the duty to take appropriate action in relation is a general obligation of SAs and is not limited to investigative and corrective powers applied in the field of data transfers.
28. In this context, the Court acknowledged the discretion of the supervisory authority to choose among adequate measures, but also clarified that the supervisory authority can be required by EU law to enforce the GDPR with all due diligence, especially where the controller or processor does not take remedial action on its own: “*Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances (...), the supervisory*

⁵ Para. 63.

⁶ Para. 107.

⁷ Para. 108.

⁸ Para. 109.

⁹ Para. 111.

authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence. In that regard, (...), the supervisory authority is required, under Article 58(2)(f) and (j) of that regulation, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.”¹⁰ Even though the judgment relates to complaints in the context of transfer of personal data to a third country, the EDPB infers that the duty to review complaints with due diligence extends to all complaints, regardless of their subject matter.

29. The Court also noted that the right of each person to an effective judicial remedy under the GDPR applies in particular where the supervisory authority fails to deal with a complaint: “*Article 78(1) and (2) of the GDPR recognises the right of each person to an effective judicial remedy, in particular, where the supervisory authority fails to deal with his or her complaint. Recital 141 of that regulation also refers to that ‘right to an effective judicial remedy in accordance with Article 47 of the Charter’ in circumstances where that supervisory authority ‘does not act where such action is necessary to protect the rights of the data subject’*¹¹.
30. In view of the relevance of national administrative laws as regards the handling of complaints, reference should be made to the jurisprudence of the Court of Justice concerning the interpretation of both national and secondary legislation including the principle of national procedural autonomy.
31. The principle of national procedural autonomy¹² implies that unless the procedural issues are directly regulated in the EU primary or secondary law, the Member States retain their competence to independently legislate on procedural issues. This autonomy has its limits as procedural solutions adopted by the Member State must be in line with principles of effectiveness and equivalence¹³. In terms of the GDPR, this means that national procedural law may not lead to fragmentation and hinder the consistent handling of complaints throughout the Union. In particular, the enforcement of the GDPR must comply with the principles of equivalence and effectiveness.
32. In C-78/98 Preston and Others¹⁴ ruling, the Court stated that: “*(...) according to settled case-law, in the absence of relevant Community rules, it is for the national legal order of each Member State to designate the competent courts and to lay down the procedural rules for proceedings designed to ensure the protection of the rights which individuals acquire through the direct effect of Community law, provided that such rules are not less favourable than those governing similar domestic actions (principle of equivalence) and are not framed in such a way as to render impossible in practice the exercise of rights conferred by Community law (principle of effectiveness) (see, to that effect, Case 33/76 Rewe [1976] ECR 1989, paragraphs 5 and 6, Case 45/76 Comet [1976] ECR 2043, paragraph 13, Fisscher cited above, paragraph 39, Case C-410/92 Johnson*

¹⁰ Para. 112 and 113.

¹¹ Para. 110.

¹² The term ‘procedural autonomy’ was used in the Court jurisprudence in Delena Wells case C-201/02, para. 65, 67, 70.

¹³ See also C-201/02, para. 70.

¹⁴ C-78/98, para. 57.

[1994] ECR I-5483, paragraph 21, and Case C-246/96 Magorrian and Cunningham v Eastern Health and Social Services Board [1997] ECR I-7153, paragraph 37)".

33. Moreover, in N.S. and Others¹⁵ case, the Court ruled that: "According to settled case-law, the Member States must not only interpret their national law in a manner consistent with European Union law but also make sure they do not rely on an interpretation of an instrument of secondary legislation which would be in conflict with the fundamental rights protected by the European Union legal order or with the other general principles of European Union law (see, to that effect, Case C-101/01 Lindqvist [2003] ECR I-12971, paragraph 87, and Case C-305/05 Ordre des barreaux francophones et germanophone and Others [2007] ECR I-5305, paragraph 28)." ¹⁶
34. The extensive case law quoted by the Court reiterates that the Court has consistently ruled that Member States must interpret and apply secondary European Union legislation in a manner consistent with fundamental rights and interpret national law in consistence with European Union law.

3 INVESTIGATING COMPLAINTS

3.1 Introduction

35. Supervisory authorities are independent public administrative authorities with specific supervisory tasks. It is an inherent feature of a supervisory authority that it has a certain margin of discretion to set its priorities in its enforcement activity while cooperating with other supervisory authorities with a view to ensuring the consistency of application and enforcement of the Regulation.
36. Complaints are one of a number of sources of information for detecting infringements of data protection rules and the handling of complaints is for that reason naturally an important task for supervisory authorities.
37. As mentioned above, the right of the individual to the protection of personal data is a fundamental right. In order to ensure the fulfilment of this right, it is of crucial importance that supervisory authorities cooperate effectively. To this end, supervisory authorities must reach a common understanding of the obligations entrusted to them by the GDPR.
38. Supervisory authorities have thus pursuant to Article 57(1)(f) a duty to handle each and every complaint submitted to them and to investigate the subject matter of the complaint to the extent appropriate. It is crucial that supervisory authorities have a shared understanding of this obligation and have efficient procedures for handling complaints.

3.1.1 The role of national procedural law

39. The current regulatory system of EU law does not aim to unify procedural law. EU legal instruments may include procedural provisions (such as the GDPR Articles conferring certain powers on supervisory authorities), but insofar EU law does not provide for specific procedural rules, national procedural law

¹⁵ C-411/10.

¹⁶ Ibid, para. 77.

applies. This is known as the principle of national procedural autonomy, which is a general principle of EU law. This general principle is limited, as is outlined extensively in the case law of the CJEU, by the EU principles of equivalence and effectiveness. These principles entail that EU law should be treated the same as national law (equivalence) and the exercise of rights conferred by EU law should not be rendered excessively difficult or practically impossible (effectiveness).

40. Since the GDPR does not further regulate the handling of complaints, the tasks entrusted to supervisory authorities by Article 57 of the GDPR should be fulfilled by relying on national procedural law, which must include – at the very least – the powers provided for by Article 58 of the GDPR. However, these national procedural rules should apply to national - and EU law alike, and must not make it excessively difficult or impossible to exercise the rights conferred by the GDPR. This applies also to the handling of complaints.
41. Different national administrative rules exist. Such differences may partly be the reason why supervisory authorities handle complaints in different ways and investigate them to different extents. Nevertheless, these differences in national procedural law can never lead to situations in which the principles of equivalence and effectiveness are undermined.
42. The GDPR creates two types of rights that it is important to distinguish between: (i) the procedural rights for complainants that a supervisory authority must respect, and (ii) the substantive rights that the GDPR creates for data subjects vis-à-vis the controller/processor. The application of national procedural law should not make it impossible or excessively difficult for a complainant to exercise its procedural rights vis-à-vis the supervisory authorities (e.g. lodging a complaint), and should also not make it impossible or excessively difficult for a data subject to exercise its rights vis-à-vis the controller/processor.

[3.1.2 Procedural rights of the complainant under the GDPR and general principles of law](#)

43. The duty of supervisory authorities to handle and investigate complaints in Article 57(1)(f) corresponds with the right of data subjects to submit a complaint pursuant to Article 77.
44. Article 77 establishes a right for every data subject to lodge a complaint with a supervisory authority and to be informed on the progress and outcome of the complaint, including the possibility of a judicial remedy pursuant to Article 78. It should be noted that Article 77 does not establish a right for a complainant to necessarily become party to the supervisory authorities' administrative proceedings against the controller. Nevertheless, national procedural law can provide such a right.
45. Article 78(1) provides the affected person (natural or legal) with a right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. The dismissal or rejection of a complaint is such a legally binding decision affecting the complainant, cf. recital 143 GDPR. Article 78(2) provides data subjects with a right to an effective judicial remedy against a supervisory authority if it does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged. This indicates a duty of a supervisory authority to inform the complainant within 3 months after the submission of the complaint about the process of handling the case unless the result of the proceeding is established. It does not, however, require the case to be closed in this tight timeframe nor to inform the complainant repeatedly every three months of the

status of the case. The complainant should, however, as indicated by Recital 141 be informed that the matter requires further investigation.

46. The Regulation strengthened the position of data subjects vis-à-vis supervisory authorities by formulating a “rights-based approach” in regard to complaints. These procedural rights would be devoid of purpose if there were not a corresponding duty of supervisory authorities to handle complaints and inform complainants of the progress and outcome of the complaint. Article 57(1)(f) must therefore be read in light of Articles 77 and 78.
47. Legally binding decisions taken by supervisory authorities should fulfill the requirements set out in Recital 129, i.e. be in writing, clear and unambiguous, giving the reasons for the measure etc.
48. Taken as a whole, the provisions in question imply that every admitted complaint that is not granted must result in an outcome specifying the reasons for the decision to enable the complainant to understand the result of his or her complaint and enabling a given competent authority to exercise its power of review.
49. For every admitted complaint - which is not withdrawn –SAs must thus provide an outcome specifying the facts and legal considerations for e.g. rejecting the complaint or dismissing the complaint i.e. not investigating it further, with a view to make it a legally attackable act.

3.2 Definition of a complaint

50. Initially, the definition of a complaint needs to be explored to ensure a common understanding hereof as a basis for the interpretation of Article 57(1)(f). The definition is also crucial as it relates to when the claim may be rejected on the basis of formally not constituting a complaint.
51. The GDPR does not explicitly define what constitutes a complaint, but Article 77 provides a first understanding in providing that *“every data subject shall have the right to lodge a complaint (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation”*.
52. Furthermore, the most relevant English meanings of “complaint” include: *“A statement that something is unsatisfactory or unacceptable”*; *“The plaintiff’s reasons for proceeding in an action”* (Oxford English Dictionary).
53. The Internal Guidance on Local Cases offers additional guidance on the definition of a complaint. It specifies that a complaint may be defined as: *“a submission to a supervisory authority by an identified natural person – or a not-for-profit body, organization or association that fulfils the conditions provided by Article 80 of the GDPR – who considers that “the processing of personal data relating to him or her infringes this Regulation”*.
54. Thus, the Guidance further underlines that a complaint is not restricted to a breach of the rights of the data subject under Chapter III of the GDPR but is, more generally, an infringement of the Regulation by a processing of the complainant’s personal data.

55. On the contrary, enquiries and “tips” are not complaints. An enquiry could be e.g. a request for advice from a controller or processor on the implementation of data protection law or a request from a natural person for advice about how to exercise his or her rights. Moreover, a suggestion made by a natural person that he or she thinks that a particular controller or processor is not compliant with the GDPR would not either be considered a complaint provided he or she is not among the concerned data subjects.
56. A complaint has to fulfil the formal conditions of the Member State where it was lodged. National requirements for filing a complaint (admissibility criteria) should not undermine the right of the data subject to lodge a complaint under Article 77, with a supervisory authority of his or her choice.
57. As regards the level of proof required to admit a complaint, it is necessary and sufficient that the complainant provides a substantiated complaint. This means that the circumstances that allegedly constitute an infringement of the GDPR must be presented in a way that the supervisory authority will be able to investigate the case. If the complainant presents circumstances that state a reason, why he or she considers that the processing of personal data relating to him or her infringes the Regulation, the complaint is substantiated. In contrast, this would for instance not be the case if the subject matter is not related to personal data. The SA should however take steps, if appropriate, to clarify the unsubstantiated issues before dismissing the complaint.

[3.3 “Investigate” the subject matter of the complaint](#)

58. The GDPR does not specifically define what constitutes an “investigation” in the sense of Article 57(1)(f). The most relevant ordinary English meaning of “investigate” is to carefully examine the facts of a situation, an event, a crime, etc. to find out the truth (Oxford Dictionary). It should further be noted that the term “investigation” has a specific definition in some Member States’ national legislation which may go further than the common understanding of what constitutes an investigation.
59. The change in wording from ‘hear claims’ in Directive 95/46 to ‘handle and investigate’ in the GDPR implies a change in the tasks of supervisory authorities. An actual investigation requires the authority to take specific actions as opposed to hearing claims that has a more passive connotation.
60. The term “to handle” should, according to an ordinary meaning of the term be understood as “to deal with” (Oxford Dictionary). This understanding is underpinned by the wording proposal of the Council to Article 57(1)(f). The change in wording from “deal with” to “handle” is presumably merely a matter of semantics. The term therefore refers to the whole procedure for dealing with or handling complaints and thus covers all stages.
61. The term “investigate” entails taking all necessary and appropriate steps with a view to resolving an issue or establishing whether an infringement has been committed and if so under what circumstances. For this purpose, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority.¹⁷ Resolving an issue could include sending a letter to the

¹⁷ CJEU, C-311/18, para. 111.

controller/processor reminding it of its duties to prompt some remedial action or settling the case amicably following action by either party to the complaint to resolve the case.

62. As stated in paragraph 54 above, for all admitted complaints that are not withdrawn, SAs must provide an outcome specifying the facts and legal considerations for e.g. rejecting the complaint or dismissing the complaint i.e. not investigating it further, with a view to make it a legally attackable act.
63. Necessary and appropriate steps encompass the measures (investigative powers) mentioned in Article 58, which include requesting information from the controller or processor, notifying the controller or the processor of an alleged infringement etc., or carrying out an audit or on-site inspection.

[3.4 Investigate “to the extent appropriate”](#)

64. Article 57(1)(f) read in conjunction with Article 77 and 78 implies an individual right to have every complaint (if admissible) handled and investigated to the extent necessary to reach an outcome appropriate to the nature and circumstances of that complaint. However, it falls within the discretion of each competent supervisory authority to decide the extent to which a complaint should be investigated. An outcome could e.g. be an establishment of an infringement, that the parties to the complaint through the intervention of the SA have settled the case amicably or, that the SA has sent a letter to the controller reminding it of its duties. It also falls within the discretion of the SA to assess and decide with all due diligence the extent to which specific investigative and corrective measures are appropriate, necessary and proportionate.¹⁸

If the supervisory authority decides not to investigate a complaint further, the complainant must be informed hereof and be provided with the rationale for concluding the investigation.

65. The term “to the extent appropriate” provides the competent supervisory authority with a margin of discretion as regards the extent or depth of the investigation needed. Which investigatory steps are to be taken, depends on both the circumstances of the specific case and the requirements under national procedural law. It is therefore not possible to formulate standardized minimum requirements regarding the duty to investigate but some degree of investigation must take place if the complainant is deemed admissible. A simple data subject rights breach may entail a very brief analysis of the documentation presented to verify the validity of the complaint. On the other hand a complex, technologically sophisticated or systemic failure could prompt a supervisory authority to deepen its investigation, namely to inspect the means and/or facilities used by the controller or processor, to ask for other public authorities to cooperate, to conduct hearings, etc. In any case, an investigation normally requires taking active steps to establish the facts and legal issues. Active steps could, but should not be limited to, in minor cases be to check whether similar complaints have been received regarding the same subject matter and same controller.
66. This discretionary power must be exercised in line with the other provisions of the Regulation and in accordance with appropriate procedural safeguards set out in Union and Member State Law, impartially, fairly and within a reasonable time. In case measures are taken, these should be appropriate, necessary and proportionate, taking into account the circumstances of the case, respect

¹⁸ CJEU, C-311/18, para. 112 and 113.

the right to be heard before a measure (that may have adverse consequences), and superfluous costs and excessive inconveniences for the persons concerned should be avoided (cf. Recital 129).

3.5 Conclusion

67. The duty to handle and investigate complaints “to the extent appropriate” entails a duty for the competent supervisory authority to investigate every complaint to the extent that is appropriate in that specific case. There are certain situations where a full-fledged investigation is not required. In the absence of further Union law on the subject, this obligation can be effectuated based on national procedural law – provided that such national rules do not render virtually impossible or excessively difficult the exercise of the rights provided for in the Regulation. Moreover, SAs should always fulfill their other procedural obligations under the Regulation, as well as adhere to other applicable rules and principles of EU law.
68. The competent supervisory authority has a discretionary power to decide upon the necessary investigatory steps to be taken, including the extent and kind of information needed in order to provide a reply to the data subject and to decide on the necessity of enforcement action. This discretionary power must be exercised with all due diligence and in accordance with the relevant provisions of the Regulation. In all cases, the competent supervisory authority must examine the factual and legal issues raised by the complainant and provide a clear and reasoned reply to the complainant as well as an outcome of the complaint. Regardless of the outcome of the complaint process, sufficient reasoning must always be provided, also in cases where the complaint is rejected and no action is taken. Such reasoning may – depending on the type and complexity of the case – be kept rather short.

4 INFORMATION RELATED TO A POSSIBLE INFRINGEMENT OF DATA PROTECTION LAW

4.1 Introduction

69. A supervisory authority may determine an infringement of data protection law either when acting upon a complaint or when acting upon its own initiative, e.g. after being “informed otherwise of situations that entail possible infringements”, as stated in Recital 131.
70. The GDPR does not define the term “infringement”. In the Guidance on Local Cases, an infringement is defined as “a violation, a non-respect of the GDPR’s provisions including both the failure to accommodate the data *subject* as well as non-compliance with other controller or processor obligations”.
71. A supervisory authority may be informed of the existence of a potential infringement of data protection law through various means. The infringement could for instance come to its attention through information received through tips from natural persons (Article 54(2)), from another supervisory authority or a public authority (Article 57(1)(h)), a body association or organization not fulfilling the conditions set out in Article 80 or from press coverage.
72. Article 57(1)(f) regulates the handling and investigation of complaints as defined in Article 77. By contrast, the Regulation does not offer comparable guidance on how supervisory authorities shall handle information received otherwise related to possible infringements of data protection law. There

are, however, provisions that suggest that supervisory authorities may also launch investigations or open enforcement actions on the basis of information not originating from complaints.

4.2 Legal Framework

73. A supervisory authority has an obligation to monitor and enforce the application of the Regulation on its territory, cf. Article 57(1)(a). Spelling out the tasks of supervisory authorities in a more detailed manner, Article 57(1)(h) provides that each supervisory authority shall on its territory "*conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority*".
74. Additionally, Article 57(1)(g) entails a task to "*cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation.*"

4.3 Conclusion

75. Since the Regulation does not entail a specific obligation to act upon information related to a possible infringement of data protection law similar to the obligation in Article 57(1)(f) regarding complaints, supervisory authorities seem to enjoy wide discretionary powers to decide when to initiate an investigation ex officio based on information received on potential infringements.¹⁹
76. When deciding whether to take action and launch an investigation based on information received, supervisory authorities should take into consideration whether there is evidence of the alleged infringement and evaluate the nature, gravity and duration of the possible infringement. If the alleged infringement is very severe, supervisory authorities would be encouraged to take action even if they have not received complaints regarding the same issue.
77. Should a supervisory authority never act on any information, no matter the seriousness of the possible infringement, it would likely not fulfil the general obligation in Article 57(1)(a). Moreover, it stems from the role as a supervisory authority and the supervisory tasks and powers that supervisory authorities should, and are expected to, assess information received on potential infringements, at least at a basic level.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

¹⁹ It should be noted that national legislation may oblige a supervisory authority to assess further information received regarding a possible infringement of data protection law.

Internal EDPB Documents



Internal EDPB Document 6/2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints

Adopted on 15 December 2020

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of contents

1	PART 1 – KEY CONCEPTS.....	3
1.2	Infringement.....	4
1.3	Amicable settlement	5
2	PART 2 – Common PRELIMINARY steps to handle a complaint or an infringement.....	6
2.1	Step 1 - admissibility of the complaint.....	6
2.2	Step 2 – Preliminary vetting	7
2.2.1	Sub-step 1 – to be applied for every cross-border incoming cases	7
2.2.2	Sub-step 2 – to be applied only for DSR-complaints.....	9

The European Data Protection Board

Having regard to Article 70 (1) (e) and 56.2 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

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

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018,

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 PART 1 – KEY CONCEPTS

1. The definitions given below are related to concepts that have not already been defined in other guidelines. The terms “*cross-border processing*”¹ and “*substantially affects*”² are therefore not defined in this section since a definition has been given in the Guidelines for identifying a controller or processor’s lead supervisory authority (WP244).
- 1.1 Complaint
2. The GDPR does not explicitly define what constitutes a complaint but Article 77 gives a first understanding providing that “*every data subject shall have the right to lodge a complaint (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*”.
3. Furthermore, the most relevant ordinary English meanings of “complaint” include: “*A statement that something is unsatisfactory or unacceptable*”; “*The plaintiff's reasons for proceeding in an action*” (Oxford English Dictionary).
4. Consequently, a complaint may be defined as a submission to a supervisory authority by an identified natural person - or a not-for-profit body, organization or association that fulfils the conditions provided by Article 80 of the GDPR³ - who considers that “*the processing of personal data relating to him or her infringes this Regulation*”.
5. It follows from the above that the definition of a complaint is not restricted to a breach of the rights of the data subject under chapter III of the GDPR⁴ but is, more generally, an infringement of the Regulation by a processing of the complainant’s personal data.

¹ Article 4(23) of the GDPR.

² Article 4(23) and Article 56.2.

³ Article 57.1(f): « *each supervisory authority shall on its territory handle complaints lodged by a data subject, or by a body, organization or association in accordance with Article 80* ».

⁴ Even if Recitals 141 and 142 emphasis on the possibility for a data subject to lodge a complaint within a supervisory authority where he “*considers that his or her rights under this Regulation are infringed*”.

Example 1

A complaint is a request from a data subject about:

- a controller's refusal to give him or her a copy of his or her personal data undergoing processing (Article 15 of the GDPR);
- the absence of an answer from a controller or processor to the natural person who exercised his or her right to rectification (Article 16 of the GDPR);
- the alleged absence or insufficiency of measures implemented by the controller or processor to ensure a level of appropriate security for the processing of his or her personal data;
- the unauthorized disclosure of his or her personal data;
- the alleged unlawfulness of the processing of his or her personal data.

Example 2

On the contrary, a complaint should not be about:

- a request for advice from a controller or a processor on an envisaged or implemented processing of personal data;
- a controller or processor's general request about the GDPR, such as an inquiry about the data protection impact assessment;
- a natural person's general request about the GDPR, such as an enquiry for advice about how to exercise his or her rights mentioned in Article 57.1(e)⁵;
- a suggestion made by a natural person that he or she thinks that a particular company is not compliant with the GDPR as long as he or she is not among the data subjects.
- cases without any reference to the processing of personal data such as disputes concerning exclusively commercial- or consumer protection matters such as a violation of the controllers general terms and conditions or violation of contracts

1.2 Infringement

6. The GDPR does not define the term "infringement" either. The most relevant ordinary English meaning of "infringement" is "The action of breaking the terms of a law, an agreement" (Oxford English Dictionary).
7. Therefore, an infringement is a violation, a non-respect of the GDPR's provisions including both the failure to accommodate the data subject as well as non-compliance with other controller or processor obligations.
8. There are the following possibilities for the supervisory authority to determine an infringement:

⁵ Article 57.1(e): "*each supervisory authority shall on its territory upon request, provide information to any data subject concerning the exercises of their rights under this Regulation*".

-) The supervisory authority may determine that there is an infringement of the GDPR when acting upon a complaint, whether the complainant explicitly states that such infringement exists, or that he or she does not ;

The supervisory authority may act upon its own motion (ex officio), e.g., after being “informed otherwise of situations that entail possible infringements”⁶ (e.g. by the press, another administration, a court, or another private company, a hint by a natural person which is however not a complaint within the meaning of Article 77).

Example 3

A supervisory authority may, during an investigation carried out on its own initiative, discover that a controller does not give the data subjects all the information provided by Article 13 of the GDPR at the time where personal data are obtained.

Example 4

A supervisory authority may be informed, through a press article, of the existence of a data breach that led to an unauthorized disclosure of personal data on Internet.

1.3 Amicable settlement

9. The GDPR does not define the meaning of the term “amicable settlement”. This expression is mentioned only by Recital 131⁷ which provides that “*the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers*”. The most relevant meanings of “settlement” are “an arrangement” and “an official agreement intended to resolve a dispute or conflict”. The adjective “amicable” means “characterized by friendliness and absence of discord” (Oxford English Dictionary).
10. Since Recital 131 refers to the “full range of powers” of the supervisory authorities, we could consider that the “amicable settlement” means the use of some of these powers which do not imply the use of corrective powers provided by Article 58.2.

Example 5

A controller or processor accepts to provide any information requested by a supervisory authority to resolve a complaint, such as clear proof that it has complied with Articles 33 and 34 of the GDPR in case of a personal data breach.

Example 6

A controller abides by the request of the data subject after the supervisory authority asks it to do so (for example with a telephone call or letter).

⁶ Recital 131 of the Regulation.

⁷ Even if Recital 131 concerns cases with only local impacts, seeking for an amicable settlement may also be a good practice when a SA is handling a case that does not fulfill the conditions laid down by article 56.2, depending on the national procedural legislation.

11. On the contrary, if the controller or processor refuses to give this information, the supervisory authority will have to order the latter to provide it. In this case the supervisory authority action cannot be viewed as an amicable settlement.
12. Other supervisory authority powers such as: carrying out investigations in the form of data protection audits, obtaining access to all personal data, or obtaining access to any premises of the controller and the processing, cannot be viewed as an amicable settlement either.
13. Although the GDPR encourages ‘amicable settlement’ by mentioning it explicitly in recital 131, it should be kept in mind that national procedural legislation may further specify how amicable settlements can be implemented in practice.

2 PART 2 – COMMON PRELIMINARY STEPS TO HANDLE A COMPLAINT OR AN INFRINGEMENT

14. This section aims to set out common preliminary handling procedures when a supervisory authority receives a complaint or detects a possible infringement. The first step is to ensure that the complaint is admissible (2.1). The second step is to verify the relevant facts of the case before introducing it in the IMI system, if necessary (2.2).

2.1 Step 1 - admissibility of the complaint

15. It will occur that a supervisory authority receives a complaint that has to be rejected on admissibility grounds. It can happen mainly in three situations:
 -) the subject matter of the complaint is clearly not related to the protection of personal data. This is the case when the GDPR does not apply, for example, because no personal data are processed. Consequently, the SA is not competent to handle such complaints.
 -) the claim is manifestly unfounded or excessive pursuant to Article 57.4 of the GDPR. A complaint is unfounded when its subject matter falls within the scope of the GDPR but obviously does not justify an action from a supervisory authority. In the same vein, a repetitive complaint can be considered as manifestly excessive and will consequently not be handled by the SA.

Example 7

The individual has submitted its request for exercising its rights to the controller less than one month ago and did not receive a reply. Even if the controller has to reply without delay, the maximum period laid down by Article 12.4 of the GDPR has not yet expired. Consequently the complaint is not admissible.

-) the claim does not fulfill the formal conditions laid down by the Member State of the SA which received the complaint. These conditions could result from a legal obligation (for example the constitutional obligation to contact any administration in one of the official languages), from other applicable legal requirements e.g. administrative procedure requirements of the relevant Member State, or from the internal rule of the supervisory authority based upon respective legal provisions (such as, in some Member States, the obligation for the complainant to supply a proof of identity).

16. The complaint has to fulfill formal conditions of the Member State where it was lodged. Consequently, if the complaint is deemed admissible by the supervisory authority which received the complaint, the LSA shall not re-examine the admissibility of the complaint, due to formal aspects. In other words, the LSA cannot reject, due to formal aspects, to handle the complaint when the formal requirements of the receiving authority have been fulfilled.
17. According to Article 56.3, "*the supervisory authority shall inform the lead supervisory authority without delay*" when it receives a case about a cross-border processing which it deems has only local impacts. Nevertheless, when a supervisory authority receives a complaint that falls within one of the first two cases (the SA is not competent or the claim is manifestly unfounded), it may reject the complaint without first informing the LSA.
18. If the complaint is rejected by the SA because it does not fulfil the formal conditions (either laid down by a legal obligation in the Member State or by the internal rule of the supervisory authority), the supervisory authority which received the complaint *shall*, as a good practice and in alignment with its national law, first inform the complainant of the missing conditions in order to enable him or her to fulfil these conditions.
19. If the complainant still does not provide these elements, the supervisory authority *may* inform the LSA which can decide to handle the case or launch an ex-officio investigation if the circumstances justify that. Informing the lead supervisory authority may be particularly important when a complaint that is otherwise unsatisfactory for formal requirements reveals a serious infringement.
20. The notification of the LSA after the case has been rejected could be done on a monthly basis about the cases that have been directly rejected by the supervisory authority.

2.2 Step 2 – Preliminary vetting

21. This subsection describes a common approach on the preliminary checks to be carried out by all SAs before introducing a case in IMI ('due diligence').
22. The first sub-step mentioned below should be carried out by the receiving SA in order to obtain the information that is necessary to make a preliminary assessment of the cross-border and possible local nature of the case. The second sub-step is only to be applied for cases relating to exercise of data subject rights mentioned in Articles 12 – 22 of the GDPR ("DSR-cases").
23. Preliminary vetting of a complaint will be beneficial regardless of the route or pathway that the particular case takes afterwards (potential amicable resolution by the receiving SA, imposing corrective measures when the case is handled locally, the cooperation procedure according to Article 60 of the GDPR), as the relevant elements shall be included in the file from an early date. The preliminary vetting procedure should be completed by all receiving SAs but the specific approach may depend on whether the controller has an establishment on the territory of that receiving SA or not.

2.2.1 Sub-step 1 – to be applied for every cross-border incoming cases

24. Upon opening a case file, the receiving SA should consult the relevant publicly available information (e.g. companies' websites, national commercial register, etc.) to obtain possible information that is necessary to make a preliminary assessment of the cross-border and, if so, local nature of a case according to the criteria set out in Internal EDPB document on handling cases with only local impacts under Article 56.2 GDPR. The receiving SA could reach out to the assumed controller, the complainant, and/or the processor to obtain the necessary information if it cannot be ascertained through public

sources. When reaching out the receiving SA can either contact the assumed controller/processor directly or contact its local establishment within the territory of the receiving SA (if existing).

25. The receiving SA could ask for example the following questions:

-) Who is the relevant controller or processor for the processing in question?
-) Is there more than one establishment of the controller or processor in the EEA?
-) If so, where is the main establishment? In other words, where is the place of the central administration or the place of the other establishment that takes decisions on the purposes and means of the processing?
-) Is the processing cross-border in nature because it is being carried out in the context of the activities of establishments in more than one Member State?
-) Is the processing cross-border in nature because it substantially affects or is likely to substantially affect data subjects in more than one Member State?

26. As the receiving SA cannot be certain at this stage whether it is a case concerning cross-border processing and whether or not the case has only local impacts, a disclaimer should be included in communications with the controller/processor stating for example that:

"We need the requested information to assess whether the processing is cross-border in nature and to determine whether the subject matter of this case has only local impacts or not. The requested information shall be used in view of preparing the case-file for a handover to the Lead Supervisory Authority if such would be necessary. This letter is without any prejudice to any later decision which could be taken by the Lead Supervisory Authority in this matter."

27. The receiving SA should then assess the response received:

-) If the controller/processor provides evidence that the processing at stake is cross-border, the receiving SA must transfer the relevant information to the LSA through IMI, regardless whether it considers that the case has only local impacts or not;
-) If the controller/processor provides evidence that the processing at stake is not cross-border, the receiving SA is fully competent to handle the case according to Article 55 of the GDPR; except if the SA receives a complaint about a non-cross-border processing that is carried out in another Member State than the SA's. In such case, the receiving SA request mutual assistance to the SA in the Member State where the processing is carried out. The latter handles the case but the receiving SA remains the interlocutor of the complainant (according to Article 77.2 of the GDPR).

Example 8

An online shop has its sole establishment in Member State A. It sells products via an internet website to only customers in Member State B. In the definition of the GDPR this is not a cross border case: Art. 4 (23) (a) does not apply because we have only one establishment. Article 4 (23) (b) does not apply because the processing does not affect data subjects in more than one Member State.

-) If the controller/processor does not respond and the receiving SA has reason to believe that the processing activity may be cross-border, the receiving SA should inform the presumed LSA of the case through IMI.

- | If the receiving SA already has sufficient information to assume with reasonable certainty the cross-border nature of the processing (cross-border or not) and the nature of the case (local or not) it can immediately proceed to upload to IMI.

2.2.2 Sub-step 2 – to be applied only for DSR-complaints

28. The application of this sub-step is limited to complaints relating to exercise of data subject rights (DSR-complaints) within the meaning of chapter III of the GDPR.
29. Upon receipt of a DSR complaint, the receiving SA may – in alignment with national administrative law – request more information from the complainant and/or the assumed controller/processor (or from its local establishment) in order to establish the facts of the case. As indicated in paragraph 26 of this guidance, a disclaimer should be included in the communications with the controller / processor. For example, the following questions could be asked (in addition to those mentioned under sub-step 1 above):
 - | Has the data subject already exercised his rights vis-à-vis the controller/processor, and if so, with what results?
 - | Does the controller/processor acknowledge having received the data subject request?
 - | Does the controller/processor have already taken (or envisages to take) certain steps to carry out the request, and if so, which steps and in which timeframe?
30. The receiving SA should then assess the response of the controller/processor:
 - | When the answer indicates that the controller has in the meantime already complied with the DSR or envisages to do so in a short timeframe, the receiving SA will request appropriate supporting evidence (if not provided already). If the controller complied with the DSR to the satisfaction of both the data subject and the receiving SA, the receiving SA should no longer inform the LSA of the DSR-case through an article 56 IMI notification, as the object of the complaint is no longer present. The receiving SA should nevertheless communicate the case and outcome to the LSA at an appropriate time for instance, on a quarterly basis (i.e.: through the voluntary mutual assistance) ;
 - | When the controller refuses for whatever reason to collaborate with the receiving SA, the latter should inform the presumed LSA of the DSR-case through IMI.
31. This second sub-step of the preliminary vetting procedure may in practice give effect to data subject rights before a case ever needs to be notified to the LSA via the IMI. This may offer a potentially quick resolution to data subjects, but even if it cannot be resolved in that manner, the preliminary vetting steps already carried out should expedite the case handling once the lead supervisory authority has been seized. If the receiving SA already has sufficient information to assume with reasonable certainty the cross-border nature of the processing and the nature of the case (local or not) it can immediately proceed to upload the case to IMI.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Internal EDPB Documents



Internal EDPB Document 1/2021 on the application of Art. 62 GDPR – Joint Operations

Review of Art. 29 WP document

Adopted on 14 January 2021

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of contents

1	INTRODUCTION	3
2	DEFINITION	3
3	PARTICIPANTS.....	3
4	PROCESS	5
4.1	Step 1 – Identification of the Supervisory Authorities participating in a joint operation.....	5
4.2	Step 2 – Issue invitation to participate to a joint operation	5
4.3	Step 3 – Agreement on the “Joint Operation Action Plan” between participating SAs.....	6
4.4	Step 4 – Nature of the powers exercised by the seconding SA(s)’s members and staff.....	6
4.5	Step 5 – Completion of a joint operation.....	7
5	RESPONSIBILITY AND LIABILITY IN A JOINT OPERATION	8
6	GENERAL TERM AND CONDITIONS BETWEEN PARTICIPATING SAs	8
6.1	General operational aspects	8
6.2	Duration of the joint operation.....	10
6.3	Confidentiality, Transparency and Publicity.....	10
6.4	Information retention and re-use	11
6.5	Language and translations	11
6.6	Costs	11
6.7	Dispute resolution	11
6.8	Withdrawal of a participant SA from the joint operation	12
7	ANNEX I: JOINT OPERATION ACTION PLAN	13
8	ANNEX II: JOINT OPERATION FLOW CHARTS.....	14
8.1	Scenario: Joint operation involving Lead Supervisory Authority	14
8.2	Scenario: Joint operation between SAs (no LSA)	15

1 INTRODUCTION

- (1) This paper focuses mainly on Article 62 GDPR. In order to integrate the provisions of article 62 with the overall provisions of the Regulation, reference is also made to the following provisions of the GDPR:

Recitals: 125, 127, 134, 138

Articles: 55, 56, 57(1)g, 60, 63, 66

- (2) This process guide is accompanied by two annexes:

- | Annex I: Contain a draft outline for a joint operation action plan.
- | Annex II: Contain a case flow diagrams illustrating of the exchanges among participating Supervisory Authorities in a joint operation in two scenarios: with and without LSA.

2 DEFINITION

- (3) A joint operation occurs where two or more SAs join forces to act toward a commonly agreed purpose. To do so, SAs make available their resources including their skills and staff.

3 PARTICIPANTS

- (4) Chapter VII provides rules on Cooperation and Consistency to ensure the consistent application of the GDPR in the Member States. Cooperation amongst Supervisory Authorities can take various forms. In accordance with the GDPR, Supervisory Authorities are at liberty to engage in one or several forms of cooperation, depending on their needs and of the goal they intend to achieve¹.
- (5) Joint operation may be conducted either by SAs cooperating on a national case (on a voluntary basis) as well as with the CSA handling a case locally pursuant to Article 56(5) or by SAs working together under the One-Stop-Shop mechanism on the impetus of the Lead Supervisory Authority:

¹ Article 61 Regulation (EU) 2018/1725 (EUDPR) provides that the EDPS shall cooperate with national supervisory authorities to the extent necessary for the performance of their respective duties, in particular by providing each other with relevant information, asking each other to exercise their powers and responding to each other's requests. See also Art. 26 of the [EDPS Rules of Procedure](#) ("Article 26 Cooperation with national supervisory authorities under Article 61 of the Regulation (referring to the possibility of joint operations between the EDPS and national supervisory authorities).

1. Joint operation between SAs cooperating on a national case pursuant to Article 55 (on a voluntary basis): the SA initiating a joint operation is at the liberty to choose to involve any other SA in the joint operation.
2. Joint operation between SAs under the One-Stop-Shop mechanism handling a case locally pursuant to Article 56(2) and 56(5).
3. Joint operation between SAs under the One-Stop-Shop mechanism pursuant to Article 56(1) (on the impetus of the Lead SA): where the joint operation targets a cross border processing of personal data, the Lead SA must seek the involvement of all SA with a right to participate.

The SAs with a right to participate are:

- The SA of a MS where a significant number of data subjects are likely to be substantially affected by processing operations.
- The SA of the MS where the Controller or Processor has establishments.

The Lead SA may contact other SAs which it may deem appropriate, including authorities that have received complaints related to the joint operation.

- (6) In any case, any other SA could be invited to participate in the joint operation if it can contribute some type of resource for the success of the joint operation.
- (7) Participating SAs must cooperate proactively to define an action plan as described in Annex I that is realistic and effective considering constraints such as resources, time, costs, etc. Thus, for example, in cases in which a large number of SAs wish to participate in the joint operation, the SAs should seek to agree on the appointment of reduced teams of personnel to carry out each specific action foreseen in the joint operation.
- (8) As Article 62 does not provide for a timescale nor for any particular method on how to organize joint operations, this process guide contains some provisions to address these aspects in item V – General terms and conditions between participating SAs and annexes I and II.

4 PROCESS

(See flow charts in annex II)

4.1 Step 1 – Identification of the Supervisory Authorities participating in a joint operation

- (9) The initiating SA communicates on the possible operation by sharing all necessary information. Joint operations are formally initiated on the EDPB IT platforms.

- (10) In response, interested SAs get back to initiating SA.

No timeframe

4.2 Step 2 – Issue invitation to participate to a joint operation

(Relevant items of the action plan in Annex I can be used as a template for an invitation to participate in the joint operation. This invitation could be sent through EDPB IT platforms).

In a cross-border processing

- (11) The LSA issues the invitation to the other SAs to participate in the joint operation, including at least those SAs having a right to participate in accordance with Article 62(2). It also responds to the requests of SAs wishing to participate.
- (12) The LSA keeps conveying basic information on the case to the SAs identified as ‘non-concerned’ in order to establish as many SA with the right to participate as possible in order to include them in the Joint operation in preparation.
- (13) In case of failure by the LSA to comply with the obligation to invite within one month² or to respond without delay to

Timeframe:
without delay
within one month

² Pursuant to article 62 paragraphs (2) and (7), when “a supervisory authority does not, within one month, comply with the obligation [to 1- invite the SA of each of those Member State to take part in the joint

<p>requests to participate, the other SA may adopt a provisional measure on the territory of their Member States – Triggering of the urgency procedure and requirement of an opinion or an urgent binding decision from the EDPB (art. 62(7) and 66 GDPR)</p>	
<p><i>In other cases (cf. art. 55 or 56(5)), the initiator of the joint operation invites any SA it wishes to involve in the operation</i></p>	
<p>(14) The initiating SA issues invitations to any SAs it wishes to involve and responds to the requests of SA(s) wishing to participate.</p>	<p>Timeframe³: within one month</p>
<p>4.3 Step 3 – Agreement on the “Joint Operation Action Plan” between participating SAs</p>	
<p>(15) SAs participating to a joint operation agree on the goal(s), nature(s), resources, duration, conditions, etc. of the joint operation action plan before it formally starts.</p>	<p>No timeframe</p>
<p>4.4 Step 4 – Nature of the powers exercised by the seconder SA(s)’s members and staff</p>	
<p>(17) For any joint operation involving direct participation of SA’s members and staff on the territory of another country, the host SA may confer the same powers on the seconder SA’s members or staff involved in joint operation as its own members and staff.</p>	

operations and 2- respond without delay to the request of a SA to participate] the other SAs may adopt a provisional measure on the territory of its Member State [...].

³ Although the RGPD does not establish a specific term for this, it is considered convenient to establish a term of one month like that established when the LSA participates in the joint operation.

<p>(18) There are two conditions to meet:</p> <ol style="list-style-type: none"> 1. The national law of the host SA allows it; and 2. The seconding SA authorizes the conferment of powers on its members and staff <p>(19) Alternatively, and for investigative actions only, the host SA may accept that the seconding SA's members and staff exercise their own investigative powers.</p> <p>(20) There are three conditions to meet:</p> <ol style="list-style-type: none"> 1. The host SA's national law allows it; 2. The conditions of national law of the seconding SAs are respected, and 3. The exercise of such investigative powers is carried out under the <u>guidance</u> and in the <u>presence</u> of the host SA (staff or members). <p>(21) In general, and especially prior to a joint operation, SAs should establish, within their respective organizations, all relevant procedures to confer powers to seconding SA's members and staff.</p> <p>(22) Joint operations involving direct participation of SA's members and staff on the territory of another country will be carried out under the guidance and instructions of the host SA. The (procedural) law applicable to joint operations is the law of the host SA's member state.</p>	<p>No timeframe</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------

4.5 Step 5 – Completion of a joint operation

<p>(23) At the completion of a joint operation, the SAs may consider sharing the results in the way they consider most appropriate, taking into account, in particular, the legal constraints applicable in the host SA Member State, whether to share information with other SAs or with the public.</p>	<p>No timeframe</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------

5 RESPONSIBILITY AND LIABILITY IN A JOINT OPERATION

- (24) The Member State of the host SA assumes responsibility, including liability, for any damage caused by the staff of the seconding SA on its territory (Article 62(4) GDPR).
- (25) In particular, the Member State of the host SA makes good any damages caused by staff of the seconding SA under the same conditions applicable to damages caused by its own staff.
- (26) The Member State of the host SA generally refrains from requesting reimbursement from any other Member State. However, the Member State of the seconding SA is under the statutory obligation to reimburse in full the Member State of the host SA in respect of any sums paid to the persons entitled as a result of damages caused by the staff of the seconding SA on the Member State territory of the host SA (Article 62(5) GDPR).

6 GENERAL TERM AND CONDITIONS BETWEEN PARTICIPATING SAs

- (27) The GDPR contains many provisions which detail the functions, competences, and powers of the supervisory authorities as well as the cooperation between them.
- (28) Article 62 together with Articles 55, 56, 57(1)g and 60, as well as Recitals 123, 127, 134 and 138 and this guide prepared by the EDPB, describe the context of joint operations with a sufficient level of detail, which makes it unnecessary to establish a specific formal agreement or MoU for each joint operation. It may be sufficient for the SAs participating in the joint operation to define a joint operation action plan using the template in annex I.
- (29) In short, the GDPR is a sufficient legal basis for the supervisory authorities, on their own, to enable and implement cooperation mechanisms and, in particular, joint operations.
- (30) Therefore, the need for further specification is limited to include only those aspects which the GDPR leaves to the free will of the parties or is strictly necessary in accordance with the applicable national laws.

6.1 General operational aspects

- (31) The GDPR considers joint operations as a cooperation mechanism including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved. This open concept allows

covering different kind of actions in a very broad sense. In fact, this guide defines a joint operation where two or more SAs join forces in order to act toward a commonly agreed purpose. In order to do so, SAs make available their resources including their skills and staff.

- (32) The participating SAs, in accordance with the provisions of Article 60 (1) and 57(1)(g), must make all necessary efforts, collaborate, and exchange all relevant information between each other, to successfully complete the joint operation.
- (33) In addition, and in accordance with Recital 125, in joint operations in which there is a lead or hosting supervisory authority, it will be essential that, in its capacity as lead or hosting authority, this supervisory authority involves and closely coordinates the rest of participating supervisory authorities in the decision-making process that must be carried out to successfully complete the joint operation. Decision making should be understood as any action or outcome that may affect the later stages of the overall procedure, including the joint operation⁴.
- (34) Each SA participating in the joint operation shall draw up and keep up to date a list of its personnel involved in the joint operation.
- (35) On-site audits or inspections are carried out in accordance with the national law of the country where the audit or inspection is realised. The host SA will be responsible for coordinating and preparing an inspection plan considering the suggestions of the supervisory authorities involved to reach a consensus. The host SA should consider the different conditions related with the validity of the evidence in accordance with the respective national laws of the participating SAs if they are compatible with the law of the host SA.
- (36) When personal data are processed in the framework of the joint operation, the participating SAs will be joint controllers for such processing since they jointly determine the purposes and means of the processing. Each participating SA will be responsible for compliance with the obligations imposed by the GDPR in relation to the personal data processed and the obligations established in Chapter III of the GDPR.
- (37) With the agreement of all participant concerned, any aspect not previously agreed upon may be agreed at any time during the joint operation, as well as any previously agreed aspect may be modified.

⁴E.g. : a supervisory authority wishes to send an inspection report that includes a legal assessment to the inspected party for feedback, but as soon as the inspected party accepts the report, the legal assessment can no longer be modified. In this scenario, the supervisory authority should have agreed on that report together with the other supervisory authorities involved before sending it to the inspected party for feedback.

6.2 Duration of the joint operation

- (38) The participating SAs will decide by consensus the dates or milestones for the beginning and end of the joint operation, as well as any subsequent updates or modifications.

6.3 Confidentiality, Transparency and Publicity

- (39) Without prejudice to the provisions established in the respective national laws, the participating SAs may agree by consensus to make public the existence of the joint operation and the information related to it.
- (40) In accordance with Article 54 (2) of the GDPR, the duty of confidentiality shall extend to all SAs staff involved in the joint operation and to all SAs which, although not directly participating in the joint operation, have access to information relating to the joint operation, such as concerned authorities.
- (41) Participating SAs will implement appropriate technical and organizational measures to ensure security in the handling and exchange of information both during the development of the joint operation and after its completion.
- (42) Participating SAs will also implement appropriate mechanisms to ensure the confidentiality of information which is subject to trade secret or intellectual property both during and after the completion of the joint operation.
- (43) Notwithstanding possible national duty to share information, participating SAs shall restrict access to information relating to the joint operation to the personnel involved in the joint operation. (*“need to know” principle*).
- (44) Participating SAs shall notify without delay any breach of the confidentiality and security measures mentioned above to the other participating SAs.
- (45) Participating SAs should assume that information shared in the framework of the joint operation may have to be disclosed in accordance with national laws. When a participating SA receives a request for access to this information, it shall inform the other participating SAs without delay and will consider as far as possible the opinion of the other participating SAs in the decision made in accordance with its applicable national laws.

6.4 Information retention and re-use

- (46) Information from a joint operation will be used for the specific investigations that led to the joint operation, provided that the information is relevant for these investigations. The participating SAs will keep the information that they incorporate in their files in accordance with their respective national laws.
- (47) In accordance with their respective national laws, the participating authorities may reuse non-personal information collected in the joint operation for other different investigations that may be carried out in the exercise of their powers. The reuse of personal information should be limited to those cases in which the Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful.

6.5 Language and translations

- (48) In each action (on-site inspection, request for information, etc.) carried out within the joint operation, the languages used will be adapted to the needs of the persons and entities affected in the joint operation: controllers, processors, third parties, data subjects, etc.
- (49) The participating SAs must agree on the working languages within the Joint Operation. Each SA, responsible for each action, will provide the necessary informal translations to share the results with the rest of the participating SAs.
- (50) Other translations (e.g.: formal translations of documents) or simultaneous interpretations (e.g.: during an on-site inspection) must be paid for and arranged by the requesting SA(s) unless otherwise agreed.

6.6 Costs

- (51) Each of the participating SAs will pay their own costs incurred for their participation in the joint operation unless a different cost sharing is agreed by the participants concerned.

6.7 Dispute resolution

- (52) To resolve possible minor disputes (for example, possible conflicts between the officials involved in the joint operation, practical or logistical problems, etc.) a contact point must be appointed by each participating SA. These contact points should act to find a solution.
- (53) All participating SAs will make their best efforts to resolve conflicts that may arise and put the joint operation at risk of viability. In the event of a conflict that makes the joint operation unfeasible, the participating SAs may use the mechanisms provided for in the GDPR, such as art 64 (2) and 66.

6.8 Withdrawal of a participant SA from the joint operation

- (54) Any of the participating SAs may decide to end their participation in the joint operation. For such withdrawal to be effective, the SA will notify the other participants in writing providing legal and/or factual reasoning or arguments for its withdrawal and sufficiently in advance and will collaborate in a loyal way to minimize the impact of its withdrawal from the joint operation.
- (55) The withdrawal of the LSA will terminate the joint operation since the CSAs will not be able to continue ex officio. For this reason, this withdrawal must be exceptional and must be based on the loss of competence as the LSA or on the cessation of the causes that led to the set up of the joint operation.

7 ANNEX I: JOINT OPERATION ACTION PLAN

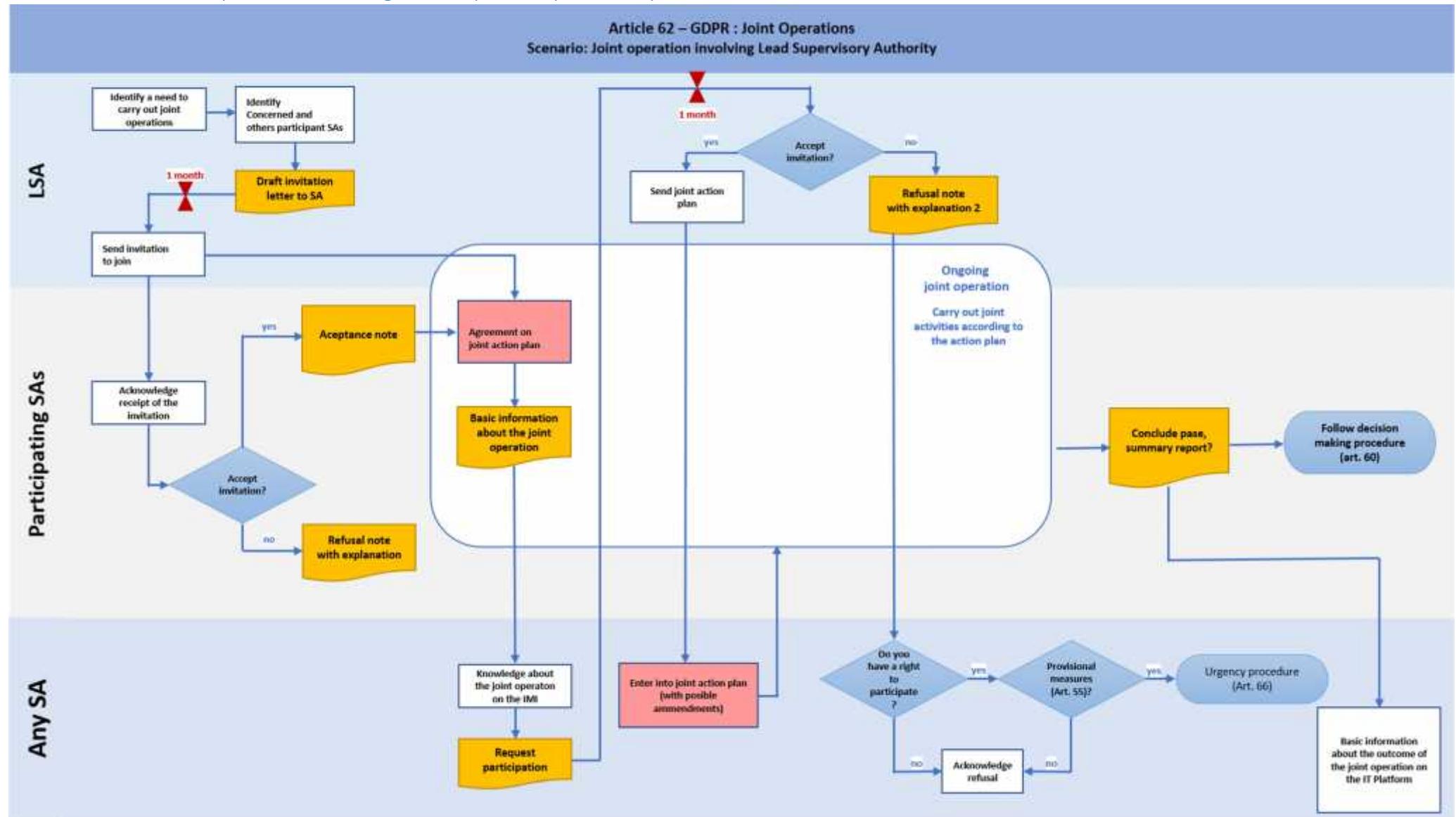
The joint operation action plan may contain:

(The existence of some specific items and, where appropriate, the level of detail, will depend on each joint operation and could be updated during the implementation of the joint operation. Participating SAs should proactively make their best to set up a realistic and effective action plan considering constraint such as resources, time, costs, etc.)

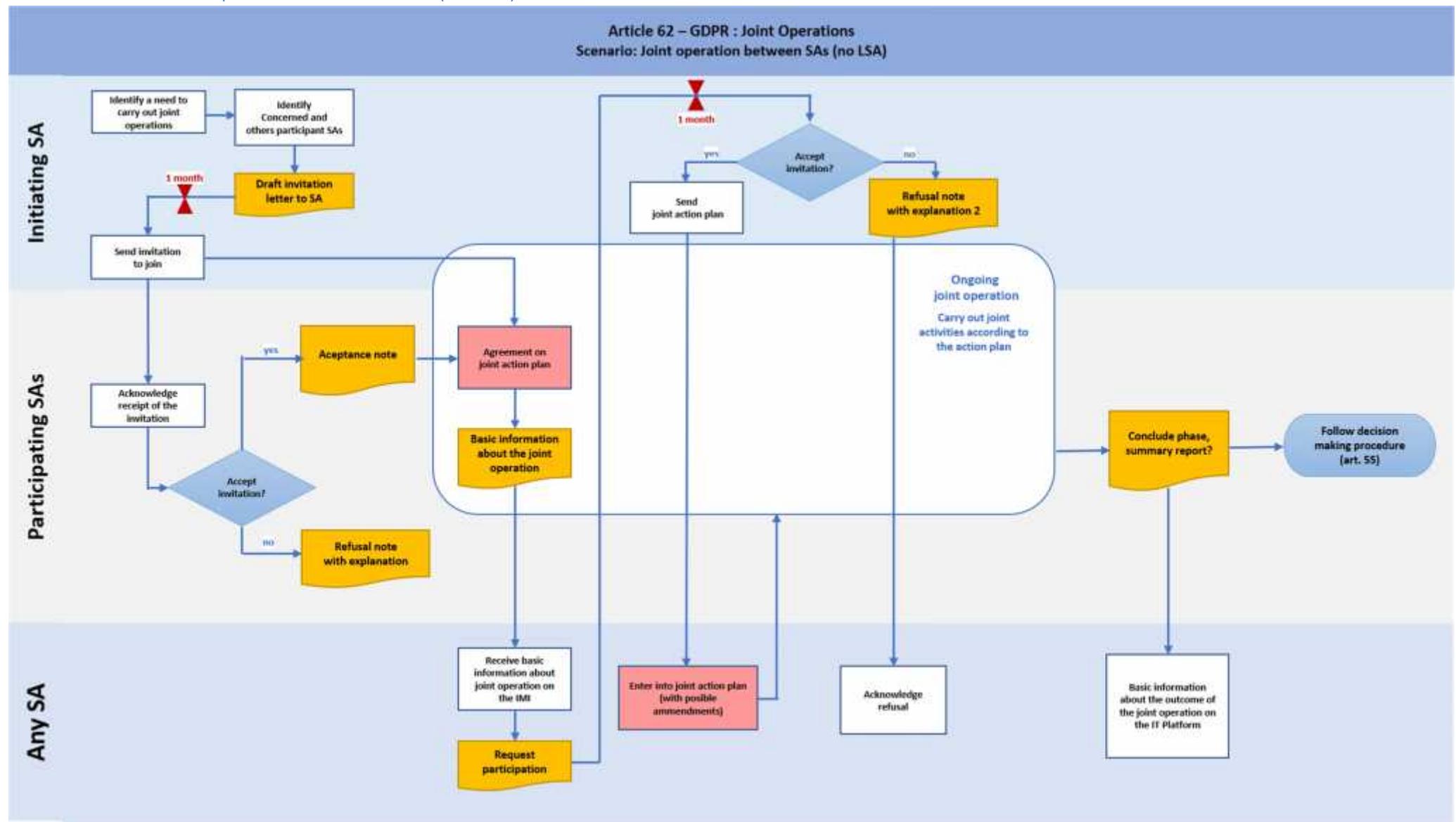
-) **Background, objective, and scope of the joint operation**
-) **Participating SAs**
-) **Dates (or milestone) of the planned start and end of the joint operation.**
-) **Staff involved in the joint operation:**
 - **People with direct participation in the joint operation: identification, roles, skills, and responsibilities**
 - **Persons authorized to participate in possible inspections or audits and if they will work under investigating power of the host SA or secondig SA**
 - **Contact points for the dispute resolution.**
-) **Joint operation planning:**
 - **Calendars**
 - **Activities**
 - **Milestones**
 - **Deliverables**
 - **Etc...**
-) **Agreed language(s) used**
-) **Cost breakdown**
-) **Confidentiality and transparency**

8 ANNEX II: JOINT OPERATION FLOW CHARTS

8.1 Scenario: Joint operation involving Lead Supervisory Authority



8.2 Scenario: Joint operation between SAs (no LSA)



Internal EDPB Documents



Internal EDPB Document 1/2020 on Art 64.1 GDPR Opinion on matters related to items on which the board has already issued an Opinion

Adopted on 18 February 2020

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

The following document outlines the approach of how to deal with a request submitted by an SA or a Member on an item on which previously a consistency Opinion has been issued. For instance, when the Board has issued an Opinion on a draft decision containing various individual items, and later a new request for an Opinion is received because the SA submits a revised draft decision (e.g. deleting or adding individual items to a DPIA list). Consideration was given to the possibility of multiple iterations of these changes.

1 LEGAL BACKGROUND

1. This raised the question of if and how the EDPB should issue an Opinion on this new draft decision while following Art 64.3 GDPR (first sentence), which states that “(...) the Board shall issue an Opinion on the matter submitted to it provided that it has not already issued an Opinion on the same matter.”
2. This provision was further enriched by Art. 10.4 of the EDPB Rules of Procedure, which specifies that “the Board may decide without undue delay and within a deadline set by the Chair, not to give an Opinion under Art. 64 (1) and (2) GDPR, because another Opinion on the same matter may have already been issued”. Therefore, this represents a threshold issue to be assessed on a case-by-case

basis. The novelty of the items submitted to the Board for an Opinion must be verified (e.g. additional items only amounting to a rephrasing of previously assessed ones probably cannot be assessed).

2 PROCEDURE

3. When it is appropriate for the Board to adopt an Opinion on the revised draft decision, a completely new Opinion is drafted, and it will be treated in the very same manner as the first Opinion. This Opinion shall in the preamble keep a reference to all previous Opinions dealing with these items to allow the tracing back of information.

Internal EDPB Documents



**Internal EDPB Document 2/2020 on how to deal with
complaints relating to data protection infringements started
before the entry into application of GDPR that continue
after 25 May 2018**

Adopted on 30 June 2020

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of Contents

1	INTRODUCTION	3
1.1	Background	3
1.2	Scope.....	3
2	LEGAL ANALYSIS	6
2.1	General context.....	6
2.2	How are cases regarding ongoing infringements dealt with in the Member States?.....	6
3	STEPS TO FOLLOW IN CASE OF CONTINUING INFRINGEMENTS RELATING TO CROSS-BORDER PROCESSING	8

The European Data Protection Board

Having regard to Article 70 (1) (e) and 56.2 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

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

Having regard to Article 3 and Article 22 of its Rules of Procedure as amended on 23 November 2018,

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 INTRODUCTION

1.1 Background

1. During its meeting on 14 May 2019, the Plenary of the European Data Protection Board (EDPB) gave mandate to the Cooperation Expert Subgroup to provide guidance on the question how to deal with cross-border complaints relating to data protection infringements started before the entry into application of the GDPR that continued after 25 May 2018.

1.2 Scope

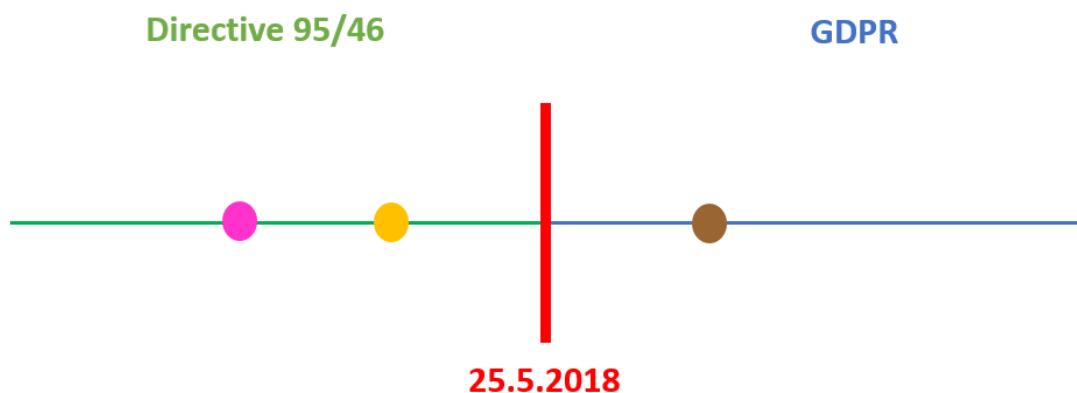
2. Many Supervisory Authorities (SAs) are dealing with complaints relating to potential/alleged data protection infringements that started before entry into application of GDPR that continue after 25 May 2018. As set out in Opinion 8/2019¹ a continuing infringement is an act (or omission) which lasts over a certain period of time².
3. The timelines below illustrate the scope of this paper (what is a continuing infringement) in case when infringement does not relate to data subject rights (case 1) and when infringement relates to data subject rights (case 2 and 3).

¹ Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment.

² See *European Court of Human Rights, Grand Chamber, case of Rohlena v. the Czech Republic, application no 59552/08*.

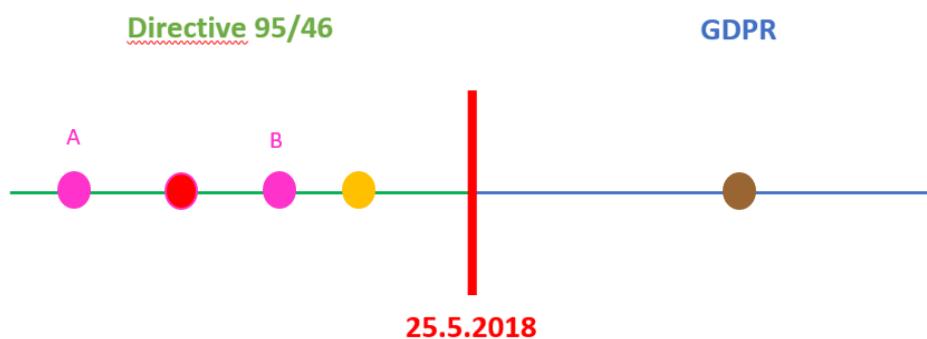
Case 1

- Complaint (not related to data subject rights) lodged before the entry into application GDPR
- Infringement starts before the entry into application GDPR
- Infringement ends after the entry into application GDPR



Case 2

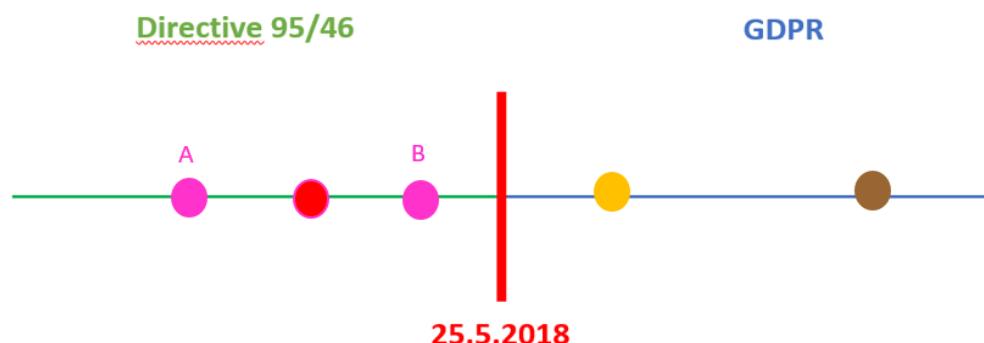
- Request for data subject right made before the entry into application GDPR
- Infringement starts before the entry into application GDPR
- Complaint lodged before the entry into application GDPR
- Infringement ends after the entry into application GDPR



4. *Scenario A:* An infringement (unlawful processing of personal data) started in February 2018. Data subject lodged a request for erasure of personal data in March 2018. The controller did not comply with the request. In April 2018 the data subject lodged a complaint with the SA. On 25 May 2018 the controller has not complied with the data subject's request yet (and proceeding has not been finished) and therefore the infringement continues.
5. *Scenario B:* The data subject made a request for access to personal data in March 2018. The controller did not answer the request made by the data subject. In April 2018 the data subject lodged a complaint with the SA. On 25 May 2018 the controller has not answered the data subject's request yet (and proceeding has not been finished) and therefore the infringement continues.

Case 3

- Request for data subject right made before the entry into application GDPR
- Infringement starts before the entry into application GDPR
- Complaint lodged after the entry into application GDPR
- Infringement ends after the entry into application GDPR



6. Scenario A: An infringement (unlawful processing of personal data) started in January 2018. The data subject lodged a request for erasure of personal data in March 2018. Controller did not comply with the request. In June 2018 the data subject lodged a complaint with the SA. On 25 May 2018 the controller has not complied with the data subject's request yet and therefore the infringement continues.
7. Scenario B: The data subject made a request for access to personal data in March 2018. The controller did not answer the request made by the data subject. In June 2018 the data subject lodged a complaint with the SA. On 25 May 2018 the controller has not answered the data subject's request yet and therefore the infringement continues.
8. As shown by the above examples, the key factor is the continuing nature of the infringement, i.e. the fact that the infringement complained against started before 25 May 2018 (the "cut-off date") and continued (was not remedied) thereafter, irrespective of the date when the complaint was lodged with the SA. However, if the processing activity affected by the continuing infringement of the controller/processor qualifies as cross-border processing after the cut-off date, the issue arises of how to arrange for the handling of a complaint regarding such cross-border processing given the distribution of competence envisaged under the GDPR. This applies in particular since competence 'for the cross-border processing carried out by that controller or processor' lies with a LSA under Article 56(1) of the GDPR as from the cut-off date, and that LSA is not necessarily the SA receiving the original complaint.
9. It should be noted that in some Member States explicit transitional provisions were put into national law to address such cases of continuing infringement. Problems might arise though on account of conflicting national provisions giving rise in cross-border cases to competence issues.

10. For such situations the guidance should seek to find proposals for practical approaches taking into account the interests of all parties involved. Though looking at how national cases are dealt with in the Member States, this guidance does not intend to give advice how to deal with purely national cases. It only applies to cross-border cases.

2 LEGAL ANALYSIS

2.1 General context

11. The handling of complaints lodged with SAs must be seen in the broader context of the GDPR as well as overarching principles of EU law. The GDPR is meant to strengthen and to set out in detail of the rights of data subjects and gives SAs the powers for monitoring and ensuring compliance with the rules for the protection of personal data (Recital 11). Ensuring consistent monitoring of the processing of personal data by SAs in all Member States is one of the most important aims of the GDPR (Recital 13, 135 GDPR) and the main task of the EDPB (Article 70 (1) s. 1 GDPR).
- According to Article 55 (1) GDPR each SA is competent to enforce the GDPR on its national territory. In cross-border cases, according to Article 56 GDPR, the authority of the single or main establishment is competent as LSA.
12. According to Article 57 (1) (a) GDPR it is the SA's duty to monitor and enforce the application of the GDPR (Recital 117 GDPR). The SA has to handle complaints lodged by a data subject and investigate, to the extent appropriate, the subject matter of the complaint (Article 57 (1) (f) GDPR). Moreover, according to Article 57 (1) (h) GDPR it is the SA's duty to conduct investigations on the application of the GDPR on their own initiative (*ex officio*).
13. It has to be kept in mind that the GDPR is of immediate effect and has priority to national Acts. Moreover, according to Recital 171³ processing already begun before 25 May 2018 should comply with the GDPR by 25 May 2018.

2.2 How are cases regarding ongoing infringements dealt with in the Member States?

14. There are different provisions in national Acts on the application of the GDPR on complaints relating to infringements that started before the entry into application of GDPR and continued after 25 May 2018.

National transitional provisions

1. In most Member States⁴, no transitional provisions apply or these provisions require the SA to apply the GDPR globally to complaints lodged before 25 May 2018 and regarding ongoing infringements. This would mean that these Member States find the one-stop-shop (OSS) mechanism to be applicable to the cross-border cases arising from pre-GDPR complaints.

³ Recital 171 s. 2 "Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force".

⁴ Such as Austria, Czech Republic, France, Germany, Italy, Luxembourg, Norway, Romania, Spain, Sweden.

- 2. However, there also exists, in some Member States, a ‘mixed’ approach in the transition provisions, where the GDPR will be applied as a substantive law to complaints lodged before 25 May 2018 with ongoing infringements, but the administrative proceeding will be governed by the previous procedural regime (Poland). Thus, the OSS mechanism would not be found to be applicable to these pre-GDPR proceedings.
 - 3. In other Member States the transition provisions require that in case a complaint is lodged before 25 May 2018 and the investigation is initiated before this date (Hungary, Slovakia), or in cases where either the request to the controller was made, the contravention occurred or the complaint has been lodged before this date (Ireland, Slovenia), the previous legal regime would apply. Consequently, for SAs of these Member States the cooperation (and consistency) mechanism does not apply.
 - 4. Regarding sanctions to an infringement that started before 25 May 2018, in many Member States according to the principle of non-retroactivity either the provisions of the previous legal regime or, in other Member States, those of the more lenient legal regime would apply.
15. In cases under 2. and 3., the receiving SA would not upload the case into the IMI system, as the OSS mechanism did not exist in previous data protection regime. On the other hand, the assumed LSA may be obliged to reject such complaint from the CSA that uploaded the case into the IMI system as it is precluded from acting as Lead Supervisory Authority (LSA). This paper focuses on the LSA’s role in this context, especially on the application of the GDPR OSS mechanism to the complaint.

National approach to data subject’s pre-GDPR and post-GDPR rights

16. SAs have different approaches to give effect to the GDPR provisions in cases where the application of the GDPR might not seem clear. When considering if there is a continuing data protection infringement, in some cases SAs take also account of the scope of the request lodged by a data subject; in particular, they consider if the right had already (similarly) existed under the previous national legal system or if it has been newly created by the GDPR.

Example 1: GDPR applied to continuing infringements that started pre-GDPR

In case of a request for access, expressly based on Article 15 (1) GDPR and subsequent complaint, both lodged before 25 May 2018, and dealt with by the SA after 25 May 2018, the complaint might be considered under GDPR if the infringement continued after that date. However, it would be taken into account that the request at the time it was lodged would not have been founded according to Article 15 (1) GDPR but according to the law previously applicable.

Counter-Example 1: Previous legal regime applied to continuing infringements that started pre-GDPR

A request for access according to Article 15 (1) GDPR lodged before 25 May 2018 and a complaint lodged before or even after this date would be treated by some SAs according to the substantive law applicable at the time of the request. However, in case the controller does not answer the request

before 25 May 2018, the SA might apply the GDPR and consider the lack of providing access an infringement of the GDPR.

17. While requests under Article 15 (1), Article 20 (1) and 21 (1) GDPR lead only to an infringement in case the request is not reacted upon properly, in other cases, e.g. in case of requests under Articles 16, 17 (1), 18 GDPR, processing of data may be without a legal basis. A controller's duty to rectification and erasure of personal data exists irrespective of the existence of a data subject's request, e.g. in case the personal data are no longer necessary to fulfil the purpose of the processing or if the retention periods have expired.

Example 2: *Ex officio* action taken in response to continuing infringements that started pre-GDPR

A request under Article 17 (1) GDPR⁵ and a complaint are lodged before 25 May 2018. In the view of some SAs a request by a data subject under Article 17 (1) GDPR, lodged before 25 May 2018 would lead to a GDPR infringement as of 25 May 2018 if it is established that the infringement continues after 25 May 2018 and the SA might, if it is not legally precluded from, consider to handle the complaint *ex officio*.

3 STEPS TO FOLLOW IN CASE OF CONTINUING INFRINGEMENTS RELATING TO CROSS-BORDER PROCESSING

18. This guidance is aimed at putting forward proposals for those cases where

- the complaint fulfils the formal conditions laid down by the Member State of the SA which received the complaint
- the receiving SA has introduced the case into the IMI system and
- the assumed LSA is precluded from declaring itself as LSA. According to its national procedural rules, the assumed LSA would either not apply the GDPR to the case at all, or not apply the procedural rules laid down in the GDPR (Articles 60 et seq. GDPR).

Example 3: OSS mechanism initiated by the receiving SA to continuing infringements that started pre-GDPR

A request according to Article 17 (1) GDPR and a corresponding complaint are lodged before 25 May 2018, and dealt with by the SA after 25 May 2018. The infringement is ongoing after 25 May 2018.

Most SAs would apply the GDPR. The controller's refusal to rectify or erase personal data would be considered an ongoing infringement after 25 May 2018. In a cross-border case the receiving SAs would start a cooperation procedure in accordance with Article 60 GDPR if the case is not a local one according to Article 56 (2) GDPR.⁶ In the latter case, the SAs would inform the assumed LSA according to Article 56 (3) GDPR.

⁵ See Art. 12 (b) of the Directive 95/46.

⁶ See in this respect also Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR and related issues such as the preliminary vetting of complaints.

Counter-Example 3: OSS mechanism not found applicable to continuing infringements started pre-GDPR

A request according to Article 17 (1) GDPR and a corresponding complaint are lodged before 25 May 2018, and dealt with by the SA after 25 May 2018. The infringement continues after 25 May 2018. SAs which, according to national law provisions, are precluded from applying the GDPR in case the request, or both, the request and the complaint were lodged before 25 May 2018, or are precluded from applying the GDPR procedural rules to complaints lodged before this date, would not initiate a procedure according to Article 60 et seq. GDPR and would not declare themselves as LSA.

19. The guidance is not giving advice on how the assumed infringement is supposed to be assessed and sanctioned by the LSA. The LSA might come to the conclusion that the complaint is unfounded or the infringement (in accordance with national procedural rules or the principle of non-retroactivity), is not to be sanctioned under GDPR. Nevertheless, the question arises of how a complaint in a cross-border case, that is found admissible by the receiving SA and introduced into the IMI system, should be dealt with.
20. It is assumed that prior to initiation of an OSS procedure, it has already been established that the infringement complained against is a continuing one. Which means that, in the meantime, there has been no reply to the request made by the data subject to the controller or there has been only a partial reply, and that the complaint lodged with the SA prior to 25 May 2018 is admissible under the receiving SA's legislation in this respect. Such an analysis is in line with best practice as outlined in the Article 56.2 internal guidance, where the receiving SA should carry out preliminary vetting of a complaint which might also include contacting the data controller or its establishment situated in the receiving SA's Member State. It might also be preferable to contact the data subject and verify whether his request had not been answered upon.
21. If the abovementioned situation takes place and it is established that the infringement is continuing, different scenarios can be envisaged depending on the national legislation the assumed LSA is required to abide by (which should be made known clearly to the receiving SA in the reply to the cooperation request):
 - a) Firstly, one should recall that Article 60 (1) GDPR obliges the LSA and the CSAs to cooperate with each other in an endeavor to reach consensus within the cooperation procedures without involving the EDPB (Recital 138 s. 2). Informal cooperation procedures should be triggered, thus, before initiating formal procedures. The receiving SA may consider contacting the data subject or the data controller in line with the preliminary vetting procedures as outlined in Article 56.2 internal guidelines.
 - b) If the assumed LSA's national legislation provides that either the request with the controller or the complaint must have been lodged with the SA after 25 May 2018, the receiving SA (CSA) should contact the complainant and invite him or her to withdraw the existing complaint and lodge a new (possibly identical) complaint with the SA and to lodge a new request to the controller. In both cases the CSA should explain the underlying reasons (related to assumed LSA's national legislation constraints) and the consequences that may occur if the data subject refuses to do so

(including the possibility of a dispute between the involved SAs to be settled by the EDPB under Article 65 (1) (b), see below). If the data subject accepts that proposal, the LSA will then act on the new complaint pursuant to the GDPR (Article 60). If the data subject does not accept the above proposal, the available options are outlined in paragraphs c) and d) below.

- c) If the data subject does not accept the proposal by the SA to lodge a new (post 25 May 2018) complaint and request in respect of a continuing infringement, it should be considered if there can be reached a consensus between the assumed LSA and the receiving SA as to whether the complaint can be dealt with by the assumed LSA *ex officio*. If the *ex officio* action cannot be followed, the assumed LSA will resolve the case in accordance with its national provisions⁷.
- d) In case the assumed LSA, according to its national procedural rules, would refuse to handle the case as a competent authority, the receiving SA can ask the EDPB for a binding decision. Pursuant to Article 65 (1) (b) GDPR where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment, the binding decision of the Board shall be adopted. This article applies to all individual cases, even those pre-GDPR with ongoing infringements, as this competence of the Board arises from 25 May 2018 onwards.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁷ For instance Section 8(2) of the Irish Data Protection Act provides: “The Act of 1988 shall apply to (a) a complaint by an individual under section 10 of that Act made before the commencement of this section, and (b) a contravention of that Act that occurred before such commencement”.

Internal EDPB Documents



Internal EDPB Document 5/2020 on how to proceed with cases under cooperation and consistency procedures in view of the end of the Brexit transition period

Adopted on 19 November 2020

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of Contents

1	INTRODUCTION	3
1.1	Background	3
1.2	Scope of the internal working document	3
2	LEGAL ANALYSIS	4
2.1	Practical Consequences.....	4
2.1.1	IMI Article 56 or 60 Procedures where UK ICO is named as LSA (complaints + investigations).....	4
2.1.2	IMI Article 56 or 60 Procedures where the ICO is a CSA, referred to other countries' SAs (complaints + investigations)	6
2.1.3	IMI Cooperation Procedures – Article 61.....	6
2.2	IMI Consistency Procedures – Article 64.....	7

The European Data Protection Board

Having regard to Article 70 (1) (e) and 56.2 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

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

Having regard to Article 3 and Article 22 of its Rules of Procedure as amended on 23 November 2018,

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 INTRODUCTION

1.1 Background

- As part of the discussion on Brexit, the EDPB Plenary meeting of 20 October 2020 agreed that the Cooperation expert subgroup ‘will develop a framework of legal and practical criteria that will serve the smooth handling of ongoing cases’ in view of the forthcoming end of the Brexit transition period (31 December 2020).

1.2 Scope of the internal working document

- This internal working document is meant to provide, in the first place, the required assessment of existing cross-border processing cases involving the UK SA as LSA in the EEA from a legal and practical perspective; to that end, the current IMI procedures involving the UK SA as LSA were considered further to analysis provided by the Secretariat.¹
- The end of the transition period means that whatever IMI procedure is ongoing as of that date, the UK SA will no longer be able to participate in it thereafter via IMI. This is why this document will also consider the options in cases where the UK SA is currently a CSA in IMI procedures.

¹ Please note that the attached analysis does not reflect the volume of complaint cases contained within each case register or voluntary mutual assistance module. The number of case registers reflects the number of entries in the IMI case register, which have been set for the purpose of handling cross-border complaints. As these entries can be used, however, for the purpose of bundling complaints, the above numbers do not necessarily reflect the total number of cross-border complaints received by the ICO from any specific SA.

When transferring complaints using an Article 61 request or notification, SAs can bundle multiple cases in a single module. As a result, the number of requests or notifications does not necessarily reflect the total number of cases transferred to the ICO by any specific authority using this method.

2 LEGAL ANALYSIS

4. The OSS mechanism relies on the EU main establishment criterion, which is dependent on factual circumstances as per the requirements of Articles 56(1) and 4(16). Accordingly, the qualifications of being LSA and CSA in the OSS may not be modified by an agreement between the involved SAs and the controllers/processors concerned. Thus, the UK SA will cease to be either a LSA or a CSA as from 31 December 2020 by definition.
5. Additionally, and as clearly set out by the WP29 in its WP244 Guidelines, '*The GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. [...] This means that controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative.*'
6. This requires breaking down the consequences of the end of the transition period on IMI procedures depending on the individual procedure and the role played by the UK SA.

2.1 Practical Consequences

7. Analysis of information provided by the Secretariat shows that there are no ongoing Article 62 and 65 or 66 procedures involving the UK SA as of 13 November 2020. The focus will be therefore on the following IMI procedures:
 - Article 56 – identifying or assuming the ICO as LSA or identifying the ICO as CSA
 - Article 60 - ongoing OSS procedures with ICO as LSA, including Case Registers
 - Article 61 - mutual assistance procedures
 - Article 64 - consistency procedures
8. Having due regard to and without prejudice to all legal rights and obligations of both the ICO and all EEA authorities, all parties are invited to carefully consider the legal and practical deadlines in the cooperation procedure under Chapter VII of the GDPR and the feasibility of progressing matters with such deadlines approaching 31 December 2020, for example with regard to registering new cases in IMI that involve the ICO or expressing objections in ongoing procedures that involve the ICO.
9. Further, all EEA authorities are invited to finalise all data exchanges with the ICO by the 31 December 2020.

2.1.1 IMI Article 56 or 60 Procedures where UK ICO is named as LSA (complaints + investigations)

10. As of 13 November 2020 there are several open Article 56 procedures to confirm the identification of the ICO as LSA, which have advanced to different degrees (some of them are still in the Article 56 stage, others have led to starting Article 60 procedures including the submission of draft decisions). In addition, SAs have transmitted complaints to the ICO identifying them as LSA using Article 61 requests in line with IMI best practice.
11. Further approaches and practices depend on whether the controller or processor has signalled to the UK LSA and to another EEA SA that another EEA establishment could become main establishment as of 1 January 2021 (scenario **(a)**) or whether there is no other establishment in the EEA that could play this role (scenario **(b)**).

12. This information should be sought as quickly as possible. A list of the pending proceedings in IMI could be used for this purpose (based on information prepared by SEC). Information received from this process should be shared with all other CSAs via an Art. 56 procedure, or else via a new Case Register entry and IC/VMN. It would be advisable to also convey the relevant information to the ICO so that the latter can provide guidance to other EEA authorities requesting it.
13. With regard to the preliminary vetting for Article 56 procedures, the CSA, in coordination with the ICO, may ask the controller's or processor's main establishment about intentions to create a new establishment within the EEA prior to the end of the transition period that can be considered the main establishment according to Article 4(16) or, if this is not the case, whether the controller/processor is going to designate a representative according to Article 27. Results of this preliminary vetting should be shared with all other CSAs via an Art. 56 procedure, or else via a new Case Register entry and IC/VMN. This is without prejudice to the controller's/processor's duty to inform the respective authority about their main establishment.

Proposed approach/best practice for (a) In case of another EEA main establishment:

14. When entering a case into IMI via Article 56, the assumed current LSA (UK) should be named as well as the assumed future EEA LSA.
15. The ICO is invited to cooperate closely with the assumed future EEA LSA, especially by means of (voluntary) mutual assistance notification and to at least transfer all relevant information to the new EEA LSA before 31st December if such LSA has been established with certainty prior to that date.²

Proposed approach/best practice for (b) In case of no other EEA main establishment:

16. Each EEA CSA will thenceforth be competent for handling the above cases at domestic level under Article 55(1) GDPR, these being no longer cross-border cases pursuant to Article 4(23) GDPR. In this case, the ICO is invited to transfer all relevant data to all EEA CSAs before 31 December 2020.
17. Notwithstanding the duties of the respective controllers, the ICO is invited to provide any information they may have to the EEA CSAs as to the appointment of a representative pursuant to Article 27 GDPR, at or prior to 31 December 2020.
18. In circumstances where the data controller has no new EEA main establishment pursuant to Art. 4(16) GDPR, the data controller is considered to be in a third country as of 1 January 2021. Further, if the data controller does not appoint an Article 27 representative, all EEA authorities as well as complainants may contact the establishment in the UK individually.

NOTE: Regarding the Article 60 procedures where UK ICO has accepted to be LSA and where draft decisions have already been inputted by ICO in IMI, they should be finalised as quickly as possible. This would be a matter of priority for the EDPB, so that precedence should be given to concluding these Article 60 procedures by 31 December via adoption of the final decision by ICO. Each EEA CSA will then continue handling the case in pursuance of the GDPR for the relevant follow-up (information to parties, appeal procedures, etc.).

² The IT Users ESG and SEC will discuss a solution to change the LSA for these Case Registers within IMI. From 2021 on, these Case Registers would then be allocated to the new LSA, which means that the new LSA would inherit editing rights from the UK DPA. This procedure should be extended, where possible, to Art. 61 procedures.

Should the ICO be unable to finalise the procedures by 31 December 2020, including on account of the objections raised by CSAs to the draft decisions, the EDPB recommends that the ICO informs the relevant EEA CSAs accordingly.

As a practical approach and in accordance with Article 77(2), the CSA should already inform the complainant that the processing might be delayed because of the shift of competence of the SA that comes with the Brexit.

2.1.2 IMI Article 56 or 60 Procedures where the ICO is a CSA, referred to other countries' SAs (complaints + investigations)

22. These procedures will continue in IMI according to OSS mechanisms, without the ICO's participation as of 31 December 2020. The OSS procedure will indeed continue in cases where several CSAs are involved in addition to the ICO, as the EEA LSA in that case is required to continue handling the subject matter of the complaint pursuant to Article 56(1) GDPR.

NOTE: The EDPB considers a matter of priority that the EEA LSA will endeavour to make available to the ICO all the information collected based on the investigations carried out until 31 December 2020, most notably when the cross-border case is based on a complaint from a UK data subject, via IMI.

24. Regarding the complaint lodged with the ICO, the ICO will proceed with handling the case in accordance with its national procedural rules.³

25. It should be recalled (see paragraph 3) that the ICO will not be regarded as a CSA from 1 January 2021 (even if it is the complaint-receiving authority) and no information exchange between the EEA LSA and ICO may take place under the umbrella of Article 60 requirements.

26. However, where ICO is the only CSA involved and accordingly the processing no longer meets the criteria as set out in Article 4(23) GDPR, no OSS procedure will exist any longer and the EEA authority that was handling the case as LSA may have discretion to continue handling the subject matter of the complaint ex officio in accordance with its national law.⁴

27. The ESG Cooperation will develop a standardised information letter which all EEA authorities may use to inform complainants residing in UK in a uniform manner.

2.1.3 IMI Cooperation Procedures – Article 61

28. Bilateral procedures, between EEA authorities and the ICO ongoing as of 31 December 2020, will be closed on that date.
29. Multilateral procedures involving the ICO as requesting authority will be closed as of 31 December 2020 as well. Multilateral procedures involving the ICO as (one of the) requested authorities will continue without the ICO's involvement. The ICO's given answers/comments will remain visible.

³ In situations where the EEA LSA has undertaken formal steps towards the exercise of corrective powers, such as issuing a notice of intent or a statement of objections, before 31 December 2020, but there is no Article 60 Final Decision yet, it is recommended that the EEA LSA engage closely with the ICO so as to avoid possible infringement of the ne bis in idem principle vis-à-vis the controller.

⁴ See footnote 3 regarding the need to engage closely with ICO in respect of these proceedings.

2.2 IMI Consistency Procedures – Article 64

30. There are currently a few procedures pending in IMI, concerning draft BCRs where UK SA is the BCR Lead.
31. Reference should be made in this respect to the recently published EDPB ‘Information Note for companies which have ICO as BCR Lead Supervisory Authority’ adopted on 22.07.2020.

For the European Data Protection Board

The Chair
(Andrea Jelinek)

Internal EDPB Documents



Internal EDPB Document 07/2020 on the Terms of Reference of the EDPB Support Pool of Experts

Adopted on 15 December 2020

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website. Some of the information in this document may not be up to date.

Table of contents

1	Terminology.....	4
2	Objectives	4
3	Scope	4
4	Support activities.....	5
5	Legal basis.....	7
5.1	Creation of the SPE.....	7
5.2	Deployment of the SPE.....	7
6	Key principles	9
6.1	Voluntary.....	9
6.2	Confidentiality and applicable law	9
6.3	Burden sharing	9
6.4	Flexibility.....	10
6.5	Coordination.....	10
7	Composition of the SPE	10
7.1	EDPB experts	10
7.2	External experts.....	11
8	Governance and management.....	11
8.1	Allocation criteria	11
8.1.1	Criteria for deployment of SPE.....	11
8.1.2	Criteria for the selection of individual experts.....	12
8.2	Requests for allocation.....	12
8.3	Allocation decisions.....	13
8.4	Selection of external experts.....	14
8.4.1	Procedure for the creation of the list of experts.....	14
8.4.2	Selection criteria to be included in the list of experts.....	14
8.4.3	Convocation.....	15
8.5	Reporting and evaluation	15
8.6	Budget and accountability.....	15
9	Financial support	16
9.1	EDPB experts	16
9.2	External experts.....	16
10	Next steps.....	16
10.1	Definition of pilot project	16

10.2	Questionnaire.....	17
10.3	Preparation of documents, templates and workflows.....	17
10.4	Network of contact points and overview of available expertise	17
10.5	Launch pilot project.....	17
10.6	Evaluation.....	17

1 TERMINOLOGY

1. For purposes of these Terms of Reference, the following terminology is used:
 - **Support Pool of Experts:** a pool of experts established in the context of the EDPB in order to assist in the carrying out of investigations and enforcement activities of significant common interest, comprising both EDPB experts and external experts.
 - **EDPB expert:** an expert employed by an EDPB member¹ or the EDPB Secretariat who is available to provide expertise relevant to an investigation or enforcement activity carried out by another supervisory authority.
 - **External expert:** an expert who is not employed by any member of the EDPB or EDPB Secretariat who is requested to provide expertise relevant to the investigation or enforcement activities of a supervisory authority against a fee, following the successful completion of the relevant selection process.

2 OBJECTIVES

2. The objective of the SPE is to contribute to a high and consistent level of protection of personal data throughout the EEA Member States by:
 - (1) **Providing material support** to EDPB members in the form of expertise that is useful for investigations and enforcement activities of significant common interest and thereby promote better protection of data subjects; as well as
 - (2) **Enhancing the cooperation** and solidarity between all EDPB members by sharing, reinforcing and complementing strengths and addressing operational needs.

3 SCOPE

3. The SPE will be deployed in order to support **investigations and enforcement activities of significant common interest** for the members of the Board.
4. Investigations and enforcement activities of significant common interest may for example concern cases involving major global companies whose activities have a substantial impact on the protection of personal data of individuals across the EEA.
5. While the need for additional support may be greatest in large and complex cases, the SPE may also be useful for smaller, yet strategically important matters. For example, there may be cases that are in first instance only of national importance, yet could set an important precedent for other EDPB

¹ For purposes of these Terms of Reference, the term “EDPB member” should be understood as referring to all EEA national supervisory authorities (including the DE Länder SAs) as well as the EDPS.

Members as regards the interpretation of the GDPR.² The complexity of the subject matter or the fact that it will be likely to be resource-intensive will, however, remain an important consideration.³

6. In other words, the possible deployment of the SPE is not limited to cases involving processing activities with EU-wide impact. Deployment in cases with primarily local (or regional) impact may also be envisaged, provided it relates to matters of significant common interest.
7. The SPE should not replace or pre-empt the ordinary discussions or exchanges that take place at the level of expert subgroups or via Confluence, where EDPB members can discuss both practical issues related to investigation and enforcement as well as matters of legal interpretation of the GDPR. For the SPE to be deployed there should also be an actual **operational need** (i.e. the supervisory authority in charge would have difficulty to proceed with its investigation or enforcement activity without receiving additional support going beyond the mere exchange of views or general discussion of the experiences from other supervisory authorities).⁴
8. **N.B.: Relationship to Coordinated Enforcement Framework (CEF):**
 - The SPE has no direct relationship with the CEF.
 - Whereas the CEF provides a framework provides a structure for coordinating recurring annual activities by EDPB members, the SPE provides a framework for sharing and combining resources.
 - Whereas the CEF identifies topics for coordinated action on an annual basis, deployment of the SPE is determined on an ad hoc (case-by-case) basis, in light of the operational needs of individual EDPB members in relation to a particular case.

It is not excluded that the SPE is deployed to support the operational needs of one or more EDPB members in the context of a particular coordinated action, to be decided on a case-by-case basis and as further specified in Section 8.⁵

4 SUPPORT ACTIVITIES

9. Supervisory authorities may require different types of expertise at different stages of their investigation and enforcement activities. As a result, there are **many different types of support** activities (types of expertise) that can be provided which include, without being limited to:

² This may be particularly relevant in the absence of relevant guidelines or other common position of the EDPB on the matter. Specific examples might include: licence plate tracking on highways, use of facial recognition in schools, use of video-surveillance cameras (so-called “dash-cams”) installed in commuters’ cars,

³ See also section 8.1 (allocation criteria).

⁴ Chapter VII GDPR sets out various mechanisms for cooperation among supervisory authorities that include a.o. exchange of information, mutual assistance and joint operations. The precise purpose and nature of the support activity will be determinative in identifying the appropriate cooperation mechanism. See also Section 5.2 (Deployment of SPE).

⁵ During the pilot phase of the SPE, it might be appropriate to consider the topics for coordinated action in the context of the CEF as relevant for the initial scope of the SPE, but this is not a requirement. As indicated earlier, the pilot project is likely to have a more limited scope at the outset, possibly also in terms of the types of cases. Once there has been a proof of concept, the deployment of the SPE should be more flexible and not limited to a limited set of topics. Moreover, we should avoid creating parallel coordination mechanisms.

- **analytical support** (e.g., sharing /explaining of a methodology for the carrying out of an inspection or calculating an administrative fine, legal analysis of a matter of EU law, a survey of the state of the art in a particular type of technology, ...)⁶;
 - assisting in the **performance findings** of a forensic nature (e.g., in the context of an on-site or remote data protection audit);
 - assisting in the preparation of **investigative reports** on the basis of evidence collected.
10. Experts can only support investigations and enforcement activities in accordance with the legislation applicable to the EDPB member responsible for the investigation or enforcement activity. Any deployment of the SPE must comply with the legal framework for the GDPR⁷ as well as any limitations imposed by national law. For example, certain national laws may preclude the involvement of external experts or subject the involvement of EDPB experts to additional conditions, depending on the precise nature of the support activity provided.⁸
11. In any event, the precise nature of the support activity (i.e., the ‘mandate’ of the expert for a particular support activity) will need to be clearly defined and agreed prior to deployment.⁹ It should also be recalled that many support activities can be provided remotely and will therefore not require physical meetings or travel.
12. The need for additional expertise is not always clear at the outset of an investigation or enforcement activity. Additional expertise may also be needed at later stages in the investigative and/or enforcement process (e.g. when preparing a fining decision; or in the context of an appeal).
13. The SPE may also have a more limited scope in terms of the types of support activities during the pilot phase (e.g. limited to the investigative phase).
14. It should be noted that the demand for certain types of expertise may be higher than for other types of expertise. For example, certain types of investigations may more easily be confronted with a lack of technical expertise, rather than legal support. It is therefore appropriate to map both the available expertise and demand for expertise, followed by a gap analysis (e.g., it could be that the greatest needs are situated in the domains of shortages of auditors and ICT-experts).¹⁰ In order to map both the available expertise and demand for expertise, a **questionnaire will be developed** and circulated among EDPB members.¹¹

⁶ Such support analytical support may also be provided on a consultative basis (as opposed to drafting of specific acts) and may relate to only one particular aspect of the investigation or enforcement action (e.g. analytical support to help correctly apply a particular fining methodology).

⁷ See also Section 5 (Legal basis).

⁸ For example, national laws may prohibit or restrict such an involvement, as evidence collection or forensic interventions may be submitted to specific national procedures. In addition, it is also important to take into account requirements concerning conflict of interests or functional separation (e.g. in terms of participation in investigation vs. enforcement stage).

⁹ See also Section 8.2 (Requests for allocation).

¹⁰ See also Section 7 (Composition of the SPE).

¹¹ See also Section 10 (Next Steps). The questionnaire will also serve to identify and assess potential limitations or obstacles to use of SPE resources at national level (e.g., as regards the use of external experts). For example, certain national laws may preclude the involvement of external experts or subject the involvement of EDPB experts to additional conditions, depending on the precise nature of the support activity provided.

5 LEGAL BASIS

5.1 Creation of the SPE

15. The legal basis for the creation of the SPE within the context of the EDPB can be found in Article 70 (1) (u) and (v) and Article 75 of the GDPR:
16. **Article 70(1)(u) GDPR** provides that the Board shall “*promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities*”.
17. **Article 70(1)(v) GDPR** provides that the Board shall “*promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations*”.
18. **Article 75** of the GDPR provides that the Secretariat shall provide analytical, administrative and logistical support to the Board and shall be responsible for the communication between the members of the Board.

5.2 Deployment of the SPE

19. The legal basis for EDPB members to contribute to and receive assistance from the SPE can be found in Articles 57(1)(g) and (t) GDPR, Section 1 of Chapter VII of the GDPR (Articles 60-62) as well as Article 61 of Regulation (EU) 2018/1725 (EUDPR).
20. **Article 57(1) (g) GDPR** provides that each supervisory authority shall “*cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation*”.¹²
21. **Article 57(1) (t) GDPR** provides that each supervisory authority shall contribute to the activities of the Board.
22. **Article 61(1) GDPR** provides that supervisory authorities “*shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.*”
23. **Article 62(1) GDPR** provides that supervisory authorities “*shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.*”
24. As indicated earlier, experts can only support investigations and enforcement activities **in accordance with the GDPR and other applicable legislation**. Much like the CEF, the SPE supports and builds on

¹² Article 61 Regulation (EU) 2018/1725 (EUDPR) provides that “[t]he European Data Protection Supervisor shall cooperate with national supervisory authorities and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA to the extent necessary for the performance of their respective duties, in particular by providing each other with relevant information, asking each other to exercise their powers and responding to each other’s requests.” See also Art. 26 of the Rules of Procedure of the EDPS, available here: https://edps.europa.eu/sites/edp/files/publication/20-06-26_edps_rules_of_procedure_en.pdf (“Cooperation with national supervisory authorities under Article 61 of the Regulation”).

mechanisms for cooperation that are in the GDPR. This means that the SPE is without prejudice to the functioning of the cooperation- and consistency mechanisms under the GDPR and the other tasks and the powers of the EDPB and EDPB members.¹³ There is also **no obligation** whatsoever for EDPB members to submit a request or offer of support via the SPE prior to initiating any of the cooperation mechanisms provided by GDPR. In other words: the creation of the SPE in no way precludes SAs from extending support to one another in any case they consider appropriate.¹⁴

25. Chapter VII GDPR sets out various mechanisms for cooperation among supervisory authorities that include a.o. exchange of information, mutual assistance and joint operations. The precise purpose and nature of the support activity will be determinative in identifying the appropriate cooperation mechanism. In practice, the involvement of EDPB experts may take the form of a sharing of information (Article 57(1)g, mutual assistance (voluntary/formal¹⁵) (Article 61), or joint operation (Article 62)¹⁶. As a result, the appropriate cooperation mechanism (i.e. the legal basis for a particular form of cooperation) will need to be determined on a case-by-case basis prior to deployment, taking into account also any limitations imposed by national law.
26. The GDPR does not contain any provisions concerning the use or possible role of external experts. The extent to which an external expert may be mandated to advise or provide support to a supervisory authority, or to perform to investigatory findings, is dependent entirely on national law.¹⁷ As indicated above, any deployment of the SPE must respect both the legal framework of the GDPR¹⁸ as well as any limitations imposed by national law.¹⁹
27. Finally, in light of the possible expenditure of EU budget²⁰, a separate administrative decision may also be necessary.

¹³ Any involvement of the SPE must therefore be mindful of the division of competences between EDPB and national SAs, making the most of the tasks and competences allocated to both. In the same vein, the establishment of the SPE shall be without prejudice to any other existing provisions or arrangements on cooperation or the setting up or operation of joint operations.

¹⁴ The SPE primarily seeks to *facilitate* the matching of available expertise with operational needs. It does not in any way prevent EDPB members and national supervisory authorities from directly providing each other with support whenever the operational need arises in accordance with cooperation mechanisms of the GDPR.

¹⁵ The ability to seek (and the obligation to give) mutual assistance applies to any case in which an SA requires the assistance of another SA for the performance of its tasks. Article 61 GDPR does not have to concern cross-border processing in order to be triggered. Article 61 GDPR can be used, for example, as a tool to share findings between the SAs involved.

¹⁶ Article 62 GDPR provides rules for joint operations by the supervisory authorities, including joint investigations and joint enforcement measures. The application of Article 62 GDPR is not limited to cross-border cases. In case of a joint operation within the meaning of Article 62 GDPR, any investigative powers conferred upon an EDPB expert may only be exercised with the approval, under the guidance and in the presence of members or staff of the host supervisory authority and insofar the law of the Member State of the host authority permits. The EDPB expert shall be subject to the Member State law of the host supervisory authority. The scope of application of Article 62 is limited to supervisory authorities. As a result, only experts employed by EDPB members can participate in Article 62 joint operations. Experts employed by the EDPB Secretariat cannot participate in Article 62 Joint Operations in the same manner as EDPB members.

¹⁷ Several SAs have the explicit possibility under their national law to be assisted by external experts.

¹⁸ See also Section 5 (Legal basis).

¹⁹ For example, certain national laws may preclude the involvement of external experts or subject the involvement of EDPB experts to additional conditions, depending on the precise nature of the support activity provided.

²⁰ See also Section 9 (Financial Support).

6 KEY PRINCIPLES

6.1 Voluntary

28. The involvement of EDPB experts or external experts requires the agreement of the EDPB member responsible for the investigation and/or enforcement activity. In case of EDPB experts, it also requires the agreement of their employer.
29. Any EDPB member may request or propose the involvement of one or more experts from the SPE to support an investigation and/or enforcement activity.
30. Experts will provide their expertise in accordance with the purpose, nature and duration of the support activity agreed by the EDPB member responsible for the investigation and/or enforcement activity.
31. Each EDPB member remains responsible for investigations and follow-up enforcement action in their respective jurisdictions.

6.2 Confidentiality and applicable law

32. Experts will be required to support investigations and enforcement activities in compliance with the legislation applicable to the EDPB member responsible for the investigation and/or enforcement activities.
33. Experts will be required to respect at least equivalent rules of confidentiality as the staff of the EDPB member responsible for the investigation or enforcement activities, which may require the signing of a non-disclosure agreement and to provide further guarantees of impartiality.

6.3 Burden sharing

34. As a general rule, all EDPB members should be willing to contribute expertise to the SPE. This principle must be understood as a willingness of EDPB members contribute to a balanced functioning of the programme and has to be applied flexibly. For instance, it does not imply that every member must offer the same number of experts every year or that each EDPB member should contribute the same number of experts.
35. During the pilot phase, each EDPB member and the EDPB Secretariat (SEC) should make best efforts to ensure that they can fulfil at least one request for support made by an(other) supervisory authority. In the longer term, it would be desirable to ensure more substantial and consistent availability of expertise. For example, each EDPB member and the EDPB SEC could strive, if possible, to ensure an availability of at least one full-time equivalent (1 FTE) expert to support investigations and/or enforcement activities meeting the criteria of the SPE, provided this is proportionate to their respective number of staff and effective capacity.²¹
36. Each EDPB member and the EDPB SEC will be asked to designate at least one contact point for the SPE, in order to facilitate information sharing and coordination relevant to the SPE (e.g. transmitting

²¹ For both EDPB members and the EDPB SEC, the ability to dedicate one or more FTE would of course require appropriate provisioning in their future budgets. The indication provided here is therefore also subject to future budget availability. It is also not necessary that the FTE relate to one dedicated staff member. For example, it would also be possible to internally assign one or more individuals, subject to availability and depending on subject matter, selected from a pool of more senior agents. It is also not required to designate individual experts by name (an indication of available expertise is sufficient).

requests for support to the right manager within the organisation, ensuring available expertise is communicated in the right manner and appropriately kept up to date).²²

37. While availability may not always be guaranteed, EDPB members should try to ensure that the relevant experts are available and can effectively provide support when their assistance is requested (subject to a reasonable timeframe following the receipt of the request).²³
38. A fair rotation of experts should be applied, meaning that efforts should be made to avoid that it would always be the same experts or authorities making available their experts in practice.²⁴

6.4 Flexibility

39. The precise purpose, nature and duration of the support activity, as well as the appropriate cooperation mechanism (where applicable), are to be determined on a case-by-case basis in writing and before the starting of the activity.
 - The appropriate mechanism for cooperation will be determined by mutual agreement between the EDPB member responsible for investigation or enforcement activity and the EDPB member(s) providing support, taking into account any additional requirements or limitations imposed by national law.²⁵
 - EDPB members may choose to request only one or a combination of several different types of support activities from the SPE.

6.5 Coordination

40. The SEC will be charged with ensuring coordination of the SPE, in accordance with Articles 70(1)(u)-(v) and 75(5)-(6) GDPR.
41. The SEC will liaise with the contact points of the SPE in order to help fill requests for support (i.e. to match experts with the operational needs articulated in the requests).
42. Templates will be created to allow EDPB members to indicate the available expertise of experts under their employ, as well to submit requests for SPE deployment in a standardised way.

7 COMPOSITION OF THE SPE

7.1 EDPB experts

43. An EDPB expert is an expert employed by an EDPB member or the EDPB Secretariat who is available to provide expertise relevant to an investigation or enforcement activity carried out by an(other) EDPB member.

²² Each EDPB Member can decide freely who it will designate as a contact point (e.g., its representative to the ENF ESG, a Head of Unit, ...), taking into account its own organisational structure.

²³ As the experts will be working on ongoing investigations and enforcement actions for their employer, they may not always be immediately available. Requests for SPE deployment should therefore envisage a reasonable timeframe (e.g. 2 to 3 months) for the time between application and expertise needed.

²⁴ Cfr. Rotation system for the Schengen evaluation – if you make available one person that should be used at least once every 2 years.

²⁵ In case of external experts, the manner in which support shall be provided shall be determined by EDPB member responsible for the enforcement activity taking into account any requirements or limitations imposed by its national law.

44. EDPB experts continue to be employed by their respective employer but provide assistance to an(other) EDPB member for the purposes, activities and duration agreed between their employer and the EDPB member responsible for the investigations and/or enforcement activity.

7.2 External experts

45. An external expert is a person who is not employed by any member of the EDPB or the EDPB Secretariat, yet has demonstrated expertise that is relevant to the needs of an investigation or enforcement activity.
46. External experts provide their services against the payment of a fee.²⁶ External experts are admitted to the Support Pool of Experts following a call for expressions of interest and the successful completion of the selection process (see section 8.4). The list drawn up on the basis of the call for expression of interest does not imply any obligation on the part of the EDPB to award a service contract (by the use of an order form) to the successful applicants.
47. The involvement of external experts may be necessary to ensure that highly specialised knowledge (e.g., in relation to forensics) can be made available to complement the expertise present in the supervisory authorities in order to address the operational needs of a specific case. As a result, external experts should only be selected on a subordinated basis and taking into account the specific needs of the requesting EDPB member, after it has been determined that no EDPB expert is available to provide the necessary support to the requesting EDPB member within the requested timeframe due to reasons of capacity.
48. In order to determine which types of expertise should be included in the call for expression of interest, it should first be assessed what expertise is available among EDPB members. Once an initial mapping of available expertise has been carried out, a gap analysis should be carried out by comparing the operational needs of EDPB members with the available expertise (e.g., it could be that the greatest needs are situated in the domains of shortages of auditors and ICT-experts²⁷).

8 GOVERNANCE AND MANAGEMENT

8.1 Allocation criteria

8.1.1 Criteria for deployment of SPE

49. The overarching criterion for allocation of SPE resources is whether or not the request concerns investigations and enforcement activities of significant common interest for the members of the Board. In addition, it should be considered to what extent the investigation or enforcement concerns matters which are complex or likely to be resource-intensive (see also section 3).
50. The EDPB PLEN may set further criteria for the allocation of experts of the SPE and possible priority areas on an annual basis, on the basis of proposals developed by the ENF ESG.
51. Absent further criteria, the following questions may be used to determine whether or not the request concerns an investigation or enforcement activity of **significant common interest**:

²⁶ Without prejudice to particular specifications agreed for a specific assignment, which will be enclosed with the request sent to the expert selected, the volumes, deadlines and remuneration for the various forms of expertise are set out in a table included with the call for expressions of interest, as well as the maximum total amount that can be paid to each individual expert.

²⁷ In this context, the gap analysis should be carried out with a sufficient level of granularity. For, example in the domain of IT there is great diversity: mainframe, oracle, java, network, security, architecture, etc..

- Does the case involves major global companies whose activities have a substantial impact on the protection of personal data of individuals across the EEA?
 - Is the possible threat to the protection of personal data likely to occur in a recurrent manner in all (or a substantial number) of Member States?
 - If it is primarily a local (or regional) case, is it a strategically important matter, i.e. that could set an important precedent for other EDPB Members as regards the interpretation of the GDPR²⁸?
52. If there is a need to choose between different actions, criteria relating to the **potential impact** will also be relevant:
- How severe is the impact of the (possible) threat?
 - Are citizens aware of the severity of this threat, and if not, should they be?
 - Is the successful completion of the enforcement activity likely to significantly improve the position (reputation) of the SAs and the EDPB as a whole? Is it likely to help demonstrate the importance of data protection for society?
53. Last but not least, deployment of SPE resources is predicated upon an **operational need**, i.e the supervisory authority in charge would have difficulty to proceed with its investigation or enforcement activity without receiving additional support going beyond the mere exchange of views or general discussion of the experiences from other supervisory authorities.

8.1.2 Criteria for the selection of individual experts

54. The selection of expert will take into account the following criteria:
- The expert meets the expectations of the requesting EDPB member in terms of expertise, availability and language spoken;
 - There is no indication of any conflict of interest²⁹;
 - In case of EDPB expert, the proposed cooperation mechanism/basis for cooperation to be applied;
 - If an external expert is proposed, it is following the determination that no EDPB expert is available and confirmation by the requesting EDPB members that the applicable legislation allows such support to be provided by an external expert.

8.2 Requests for allocation

55. Any EDPB Member seeking to make use of SPE resources submits a request to the EDPB SEC. Requests for allocation of members of the SPE should indicate:
- the purpose of the request (i.e. subject of the investigation/enforcement activity);
 - a justification of the need to make use of the SPE (such as substantiating the existence of a significant common interest as well as substantiating why the request meets the priorities/criteria as set by the EDPB);
 - A justification of the operational need;

²⁸ This may be particularly relevant in the absence of relevant guidelines or other common position of the EDPB on the matter. Specific examples might include: licence plate tracking on highways, use of facial recognition in schools, use of video-surveillance cameras (so-called “dash-cams”) installed in commuters’ cars,

²⁹ It should however be born in mind that the duty of cooperation and of confidentiality provided by the GDPR, as well as the procedures foreseen to allow cooperation between DPAs, imply there is no risk of conflict of interests simply because an employee of a SA who provides support as an EDPB expert to another SA , even if the investigation or enforcement activity eventually leads to an application of the dispute resolution mechanism.

- whether either only support from EDPB experts is sought, or whether the support may also be provided by external experts in case no EDPB members is available;
 - the nature of the expertise requested (e.g., legal advice, specific technical findings, specific form of auditing expertise, ...) from an EDPB expert or from an external experts in case no EDPB members is available;
 - where reliance on EDPB experts is envisaged: the proposed cooperation mechanism/basis for cooperation (e.g. whether the requesting supervisory authority is seeking support in the form of a joint operation, mutual assistance or sharing of information)³⁰;
 - the envisaged duration of the activity;
 - an estimation of the time to be allocated (expressed in person months or days);
 - whether physical presence of the expert is required for any of the relevant support activities and its duration; and
 - the request as regard language spoken by the expert and whether any translations of the expertise provided will be necessary (in particular into language of the national proceedings).
56. Each EDPB Member may also request the EDPB SEC to informally assess the suitability of the request and advise on a possible approach. The EDPB SEC may also liaise with contact points as appropriate (e.g. to obtain further clarification regarding the expertise that is available).

8.3 Allocation decisions

57. The decision to allocate SPE resources will be made a by a Selection Panel, which consists of three EDPB members. In order to gain experience and ensure continuity, the Selection Panel will initially be composed of the EDPB Chair and the two Deputy Chairs. Two additional EDPB members will be designated as alternates, who may substitute the either the EDPB Chair or Deputy Chair.
58. Once a request for involvement of the SPE has been submitted, the SEC assesses the eligibility of the request on the basis of the allocation criteria (point 9.1) and informs the Selection Panel of its assessment. If the Selection Panel agrees that the request concerns a case of significant common interest, the SEC circulates the request to all contact points with a view of seeking relevant experts. Communication of a call for experts may take place via Confluence.
59. In case one or several EDPB experts volunteer, the SEC will, together with the supervisory authority requesting assistance, assess the suitability considering the request made. The requesting authority will confirm that the proposed expert(s) meet its needs and that there is no appearance of conflict of interest. Based on the information received, the EDPB SEC will prepare a file for final approval by the Selection Panel, as well as the EDPS Budget Authorisation officer³¹.
60. If no EDPB experts volunteer, an assessment will be made whether any of the external experts who have successfully completed the selection process may be of assistance, provided that the supervisory authority responsible for the investigations and/or enforcement activity indicated that the support may also be provided by external experts in case no EDPB experts are available. The SEC will, together with the supervisory authority requesting assistance, assess the suitability of the external expert(s)

³⁰ The EDPB members concerned remain responsible for implementation of the formal modalities to apply those cooperation mechanism, taking into account the internal guidance documents as well possible templates developed in the context of the ENF and COOP ESG, as well as any additional requirements imposed by applicable (national) law. Where templates are used, duplication should be avoided.

³¹ Idem.

considering the request made. The requesting authority will confirm that the proposed expert(s) meet(s) its expectations in terms of expertise, availability and language spoken; and that there is no appearance of conflict of interest³².

8.4 Selection of external experts

8.4.1 Procedure for the creation of the list of experts

61. External experts are admitted to the SPE following a call for expressions of interest and the successful completion of the selection process.
62. Applicants will be invited to apply for one or several specified areas (to be specified by the applicant when expressing their interest), such as:
 - branches of law (e.g. data protection law, European Union law, administrative law,);
 - technical expertise (e.g., web tracking measurement, cryptography, privacy-enhancing technologies, ...);
 - auditing; or
 - forensics.
63. The specific areas that will be identified in the call for expressions of interest will be determined on the basis of the gap analysis between the available expertise and demand for expertise (on the basis of the questionnaire to be circulated to EDPB members).
64. On the basis of the applications received, a list will be drawn up of experts who meet the criteria. The list of experts will be valid for a period of four years from publication in the Official Journal. Inclusion in the list of external experts does not imply any obligation on the part of the EDPB to award a service contract (by the use of an order form) to the successful applicants.
65. New calls for expressions of interest, in one or more specified areas, may be issued on an as-needed basis.
66. The SEC will be charged with issuing the call for expressions of interest, receiving applications and publishing the list of external experts.³³

8.4.2 Selection criteria to be included in the list of experts

67. The specific selection criteria to be included in the list of experts will be set out in the call for expression of interest. Generally speaking, experts will be selected for the list of external experts on the basis of their professional and technical ability to carry out the tasks described. In order to be placed on the list of external experts, the applicant will:
 - have a sound professional background, with at least seven years' professional experience, including at least five years clearly related to the area of expertise in question;³⁴

³² Idem.

³³ In accordance with the Financial Regulations, the call should remain open for new expressions of interest throughout the implementation period.

³⁴ Documents required to provide evidence of their ability, skills, experience and competence for performing the work by means of: a motivation letter of no more than two pages (max. 500 words), in which the applicant sets out on his/her reasons for applying and the principal reasons why he or she should be admitted; a full curriculum vitae specifying relevant qualifications and background, relevant expertise and experience, and knowledge of languages, as well as, in annex, a copy of the most relevant certificates, namely university degrees and language

- have distinguished themselves professionally and/or academically in the branches areas relevant to the call for expression of interest (evidence, for example, in membership of networks of experts, certifications, awards, publications, etc.);
 - have an excellent written and verbal command of the English language or the language of the Member State requesting support³⁵;
 - have the economic and financial capacity to provide the services in question (i.e. be able to ensure continuity throughout the duration of the assignment).
68. The expert must notify the SEC of any previous services performed for national and international public or private entities, including European Union Institutions and Agencies, in the past five years, in the area which is the subject matter of the request.
69. When carrying out each specific expertise the expert may not be affected by any conflict of interest, within the context of a specific request, arising in particular from any economic interests, from political or national associations, from family or other personal links, or from any other relationships or common interests.

8.4.3 Convocation

70. The Selection Panel will ensure that expertise is commissioned in a fair manner on the list based on the applicants' professional profiles, taking into account the support activities requested, based on the recommendation provided by the EDPB SEC.
71. Whilst maintaining the principle of selecting the most qualified experts, the Selection Panel will ensure obtain a balance in accordance with the principles of non-discrimination, equal treatment and absence of conflict of interest.

8.5 Reporting and evaluation

72. For each allocation of SPE resources, a report shall be made up by the EDPB member responsible for the investigation or enforcement activity, documenting the allocated resources (human and financial) providing an evaluation of the support provided³⁶.
73. The SEC will provide regular reports (minimum twice a year) at the level of the ENF ESG and at PLEN level. For example, in case the number of requests risks to exceed available resources, the Plenary may be informed to help determine priorities, taking into account also the resources that remain for the relevant period.
74. The SEC will also make an annual evaluation report of the SPE initiative. For assisting the SEC in its tasks, all the EDPB members will contribute to this evaluation by completing a survey. As part of the evaluation, particular attention will be made to whether there may be ways in which to simplify the governance and management of the SPE.

8.6 Budget and accountability

diplomas; a full record of publications or writing samples on the subjects relevant to the call for expression of interest, differentiating between general publications and texts published in peer-reviewed journals and/or monographs accepted for publication after a similar review process. Where appropriate, the call for expression of interest may include specific further requirements for professional experience, similar to the one for language requirements.

³⁵ The call for expression of interest may include specific further language requirements for written expertise.

³⁶ A template may be provided by the EDPB SEC.

75. The funding of eligible expenses of the SPE will be part of the EDPB budget³⁷. The decision to support a particular investigation or enforcement activity will be taken by the Selection Panel, with the additional agreement of the EDPS Budget Authorisation officer.

9 FINANCIAL SUPPORT

9.1 EDPB experts

76. The salary of EDPB experts remains covered by their employer, as they remain part of the staff of their employer. Each EDPB Member as well as the EDPB SEC will therefore need to consider this in their respective budget plans.
77. Upon confirmation of eligibility, the EDPB may, subject to budget availability, assist by reimbursing the costs of two common areas of expenditure:
- (1) travel and, subject to further assessment, accommodation and/or daily allowances (in case physical presence is required)³⁸,
 - (2) translation (e.g., of investigative reports) in specific cases.³⁹

9.2 External experts

78. Upon confirmation of eligibility, the EDPB may assist by reimbursing the costs relating to travel and daily allowance (in case physical presence is required).
79. Fees of external experts may also be eligible for reimbursement, subject to budgetary availability and approval of the EU Budgetary Authority as regards allocation of EDPB Budget and provisioning of the necessary financial resources.⁴⁰ Contact may also be made with the European Commission in case the SPE could also rely EU funding programmes (e.g., in the form of a project grant).

10 NEXT STEPS

80. Upon approval of the present Terms of Reference, the following steps are envisaged:

10.1 Definition of pilot project

³⁷ The EDPB Secretariat will plan for the inclusion of additional budget for SPE in the preparation of 2022 Budget that will be carried out beginning of 2021.

³⁸ It should be noted that, depending on the nature of the investigation, experts may also be able to contribute remotely and therefore their involvement does not necessarily require a physical presence.

³⁹ While the working language of the EDPB remains English, it may be necessary to translate official investigative reports into the language employed by the supervisory authority in charge of the investigation. In addition, it cannot be excluded that certain EDPB experts are not proficient in English. As a result, at most two translations can be provided: (1) into English; (2) into the language of the enforcement proceedings. However, English being the working language of the EDPB, priority should still be given to the use of English as working language. An appropriate language policy will need to be developed when it comes to the support of translation costs, subject again to budget availability.

⁴⁰ Any expenditure of EDPB Budget must occur in accordance with the relevant financial regulations and guidelines applicable to EUIs. The procedure with a call for expression of interest described in this document is premised on the assumption that external experts will only apply as natural persons and the total amount of payments remains below the threshold of the Directive on public procurement (2014/24/EU), which then allow for exception from normal procurement procedures.

81. During the pilot project, the SPE will be limited to EDPB experts.
82. The precise scope of the pilot project is still to be determined, both in terms of
 - types of cases (e.g. by focusing first on smaller yet strategically important cases or on a limited set of topics); and/or
 - in terms of the types of support activities (e.g. limited to the investigative phase).
83. To be discussed at the level of the ENF ESG and submitted for approval by PLEN.

10.2 Questionnaire

84. Development of a questionnaire to map both the available expertise and demands for additional expertise among EDPB members, to be circulated among and completed by EDPB members. The questionnaire will also seek to identify and assess potential limitations or obstacles to use of SPE resources at national level (e.g., as regards the use of external experts).⁴¹
85. Gap analysis (between available needed expertise and needed expertise) and determination of relevant criteria (including areas of expertise) for the call for external experts.

10.3 Preparation of documents, templates and workflows

86. Prepare documents necessary to administer requests for support (forms/templates), reimbursement, etc.

10.4 Network of contact points and overview of available expertise

- Identification of contact points by EDPB members
- Specification of FTE experts available for SPE pilot project deployment

10.5 Launch pilot project

87. The initial pilot project will be launched in 2021. In parallel to the pilot project, a first Call for Expression of interests for external experts will be launched, taking into account the outcome of the gap analysis in step 10.2.

10.6 Evaluation

88. After one year, the functioning of the SPE will be evaluated. The annual evaluation report will be prepared by the EDPB SEC, on the basis of the reports submitted and a survey that will be circulated for completion by all EDPB members.

⁴¹ The questionnaire should address questions such as

- What different types of support activities (types of expertise) can be made available by your supervisory authority to support the investigations or enforcement activities of other EDPB members?
- For which types of type of expertise does your supervisory often experience an operational need which can not easily be met by your current employees?
- To what extent do national laws either explicitly authorise or preclude involvement of external experts?
- etc.

Internal EDPB Documents



Internal EDPB Document 3/2021 providing guidance on the planning and preparation of EDPB Binding Decisions under Article 65(1)(a) GDPR

Adopted on 13 April 2021

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of contents

1	Planning.....	3
2	Preparation of the draft EDPB binding decision.....	3

The European Data Protection Board

HAS ADOPTED THE FOLLOWING INTERNAL DOCUMENT

1 PLANNING

1. In order to ensure the timely adoption of the binding decisions of the Board, the Secretariat should plan the work on the drafting and discussion of the draft binding decision. In principle, the Secretariat will communicate a draft planning to the Chair and the members of the Enforcement Expert Subgroup (ENF ESG) within one week after the file has been declared complete and the subject matter has been referred to the EDPB.
2. The draft planning should generally include:
 - _) the date(s) of the Plenary meeting(s) during which the binding EDPB decision should be adopted;
 - _) an indicative date of completion of the initial assessment of whether the objections meet the threshold of Article 4(24) GDPR and the date(s) of discussion with members of the relevant expert subgroup (in accordance with the decision of the Chair);
 - _) an indicative date of completion of the assessment of the objections meeting the threshold of Article 4(24) GDPR and of the substance of the case and the date(s) of discussion with members of the relevant expert subgroup(s) (in accordance with the decision of the Chair);
 - _) any further meeting dates of the relevant expert subgroup (including any extraordinary meetings of the expert subgroup(s), where appropriate and as agreed with the coordinators).
3. The draft planning may also (be updated to) include reference to possible SAESG meetings to enable a high-level exchange on matters having significant impact on the drafting process, where appropriate.
4. The draft planning should also include the evaluation of the need to redact elements or portions of the final EDPB binding decision on the basis of EU law obligations of professional secrecy to avoid any undue delay in publication.

2 PREPARATION OF THE DRAFT EDPB BINDING DECISION

5. According to Article 11(5) of the EDPB Rules of Procedure (“RoP”), the binding decisions “*shall be prepared and drafted by the secretariat and, upon decision of the Chair, together with a rapporteur and expert subgroups members*”.¹ Therefore, the EDPB Secretariat should act as lead rapporteur and the Chair should decide on the involvement of an expert subgroup and of co-rapporteurs.
6. As soon as the LSA has submitted the matter to the EDPB for dispute resolution, the Secretariat should start the assessment of the completeness of the file. During this assessment, the Chair is invited to decide on the possible involvement of co-rapporteurs and will invite EDPB members to express an

¹ See also Article 75(6)(g) GDPR, which provides that the Secretariat shall be responsible in particular for the preparation, drafting and publication of decisions on the settlement of disputes between supervisory authorities.

interest to become co-rapporteurs (unless the Chair decides not to involve co-rapporteurs for this case)². In order to ensure fairness and impartiality, the (group of) co-rapporteur(s) should not include delegations from either the LSA or CSAs that submitted objections in relation to the draft decision³.

7. Due to its expertise and due to the subject matter, the ENF ESG will generally be the subgroup involved in the discussion and work on binding decisions pursuant to Article 65(1)(a) GDPR. Depending on the agenda of the ENF ESG, the discussions related to the draft binding EDPB decision may also take place in the context of extraordinary meetings of the ENF ESG so as not to unduly disrupt the execution of the workplan of the ENF ESG or with an ad hoc format of the ENF ESG dedicated to a Article 65(1)(a) procedure⁴.
8. Finally, it should be noted that the Chair may also decide to involve the members of one or more other expert subgroups, depending on the needs of the case.
9. The Secretariat, together with the co-rapporteur(s) if applicable, should work on the preparation of the draft binding decision and regularly submit discussion points and/or draft decisions for discussion at the meetings of the designated expert subgroup. The discussion at subgroup level should aim at ensuring that the substance of the case is examined and that the direction of the work is shared by a majority of delegations and at resolving any outstanding issue.
10. The Secretariat and the co-rapporteurs, if any, should identify the views shared by the majority of the members during the discussions and take them into account.
11. As indicated earlier, Article 11(2) RoP states that the EDPB shall take into account *only* the documents which were provided by the LSA and the other CSA(s) once the matter is referred to the EDPB. This means that the LSA or CSA(s) cannot during the drafting stage introduce new elements of fact supporting their respective positions. Both the LSA and CSA(s) may of course explain and defend their respective positions during the discussions within the expert subgroup and clarify their respective positions and share their views as members of the EDPB, without introducing new information which was not already provided at the moment when the matter was referred to the EDPB.
12. In accordance with Article 76(1) GDPR, discussions of the Board and of expert subgroups shall be confidential when they concern the consistency mechanism⁵. Moreover, an obligation of professional secrecy is also imposed on the staff of all EEA national supervisory authorities⁶, the EDPS and the EDPB Secretariat⁷. This means that the duty of confidentiality and professional secrecy, which is of paramount importance, shall be respected by the EDPB and its members also in relation to Article 65(1)(a) dispute resolution cases. This concerns both the discussions and the documents exchanged.

² If the call for expression of interests to serve as co-rapporteur is made prior to the assessment that the file is complete, care should be taken not to disclose any elements of the file until after the assessment has been made and the subject matter has been referred to the EDPB.

³ See also the Judgment in *Dr. August Wolff GmbH & Co. KG Arzneimittel*, Case C-680/16 P, 27 March 2019, ECLI:EU:C:2019:257, paragraphs 29-41.

⁴ Whilst assessing the completeness of the file, the Secretariat may consult with the coordinators of the ENF ESG to assess whether it is necessary to establish an ad hoc format of the ENF ESG dedicated to a Article 65(1)(a) procedure.

⁵ Article 33 RoP.

⁶ Article 54 (2) GDPR.

⁷ Article 56 of Regulation (EU) 2018/1725.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Internal EDPB Documents



Internal EDPB Document 3/2019 on Internal guidance on Article 64 (2) GDPR

Adopted on 8 October 2019

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of Contents

1	INTRODUCTION	3
1.1	SCOPE	3
1.2	GENERAL CONTEXT AND RATIO OF ARTICLE 64 (2) GDPR.....	3
2	REQUESTS UNDER ARTICLE 64 (2) GDPR	4
2.1	ARTICLE 64 (2) GDPR	4
2.2	CONDITIONS OF ARTICLE 64 (2) GDPR	4
2.2.1	What is a “matter of general application”?	4
2.2.2	What is a “matter producing effects in more than one Member State”?	5
2.2.3	Relationship between both conditions	6
2.2.4	Relationship to cooperation procedures (Article 60 et seq. GDPR)	6
2.3	ADMISSIBILITY REQUIREMENTS (ARTICLE 64 (2) GDPR)	8
2.3.1	Possible applicants	8
2.3.2	Substantive requirements	8
2.3.3	Written reasoning	8
2.3.4	Exception from the right to obtain an opinion.....	8
2.4	CONSEQUENCES	9
2.5	OUTLOOK.....	9

The European Data Protection Board

Having regard to 64.2 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

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

Having regard to Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 INTRODUCTION

1.1 SCOPE

1. During its meeting on 5 July 2018, the Plenary of the European Data Protection Board (EDPB) gave mandate to the Cooperation Expert Subgroup to analyze the scope of Article 64 (2) and to provide guidance on the practical application of Article 64 (3) last sentence of the General Data Protection Regulation (GDPR), including possible implications for the Rules of procedure (RoP) of the EDPB.
2. ***While the second part of the mandate, i.e. the guidance on the practical application of Article 64 (3) last sentence GDPR, including possible implications for the RoP of the EDPB will be realized in a separate document, this document intends only to analyze the scope of Article 64 (2) GDPR.***

1.2 GENERAL CONTEXT AND RATIO OF ARTICLE 64 (2) GDPR

3. The provision at stake, namely Article 64 (2), must be read in a broader context. Placed in the middle of Chapter VII entitled "Cooperation and Consistency", the purpose of Article 64 in its entirety is to ensure a coherent and common interpretation and application of GDPR.¹ Ensuring consistent monitoring of the processing of personal data by Supervisory Authorities (SAs) in all Member States is one of the most important aims of the GDPR (Recital 13, 135) and the main task of the EDPB (Article 70 (1) s. 1). By determining clear competencies (Articles 55, 56) and procedures (Articles 60 et seq.) the GDPR enables SAs to achieve a consistent and high level of protection of personal data across the European Union (EU) and the European Economic Area (EEA).
4. In this regard, the GDPR foresees different tools which are available for the SAs to obtain a consistent application and interpretation of the GDPR. As an example can be cited the One-stop-shop mechanism laid down in Article 60, but also the possibility to ask other SAs for mutual assistance (Article 61 GDPR) or to conduct joint operations (Article 62 GDPR). In case of disagreement concerning an individual case, Article 65 provides for the possibility to adopt a binding decision within the EDPB.

¹ See in this regard also Article 63.

5. Article 64 for its part provides the possibility to request an opinion from the EDPB. While requesting an opinion from the EDPB is obligatory in the specific circumstances mentioned in Article 64 (1), Article 64 (2) provides SAs, the Chair of the EDPB and the European Commission with the possibility to request an opinion from the EDPB regarding matters of general application or producing effects in more than one Member State. As such, Article 64 provides SAs with a valuable tool to ensure the consistent application and a high level of protection of personal data in the EU.
6. Consequently, it results from the above - and should be kept in mind while interpreting Article 64 (2) - that this provision aims, among all the others mentioned above, at ensuring harmonious interpretations of the GDPR.

2 REQUESTS UNDER ARTICLE 64 (2) GDPR

2.1 ARTICLE 64 (2) GDPR

Article 64 (2) GDPR:

*"Any supervisory authority, the Chair of the Board or the Commission may request that **any matter of general application or producing effects in more than one Member State** be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62."*

7. In contrast to Article 64 (1) the GDPR does not provide an obligation for the SA, the Chair or the Commission to ask for an opinion in the context of Article 64 (2). Consequently, it remains at the discretion of the possible applicants to request such an opinion. However, this possibility to request for an Opinion of the EDPB only exists if one of the two conditions is met, namely if the request concerns a matter of general application or a matter producing effects in more than one Member State.

2.2 CONDITIONS OF ARTICLE 64 (2) GDPR

8. The legislator laid down two different conditions. The distinction and relation between those conditions is explained further below.
 - 2.2.1 What is a "matter of general application"?
9. A matter of general application concerns abstract questions regarding data processing that has the potential to infringe the fundamental right to data protection. Consequently, a matter of general application can first of all refer to the interpretation of provisions of the GDPR.
10. Such abstract legal questions may arise without a specific triggering event but also from an ongoing case, for instance where it is necessary to constitute a precedent. When a question of interpretation, which is new, and/or of general interest for the uniform application of the GDPR is raised, or where the existing case law and previous opinions and decisions by the EDPB do not appear to give the necessary guidance to deal with a legal situation, it is useful for SAs to have a tool which permits to

obtain a general solution for the question at hand. This also contributes to consistency as all SAs are involved in the Article 64-procedure.

11. A matter of general application can also refer to questions related to the practical implementation of the GDPR. This includes abstract procedural questions regarding the cooperation and consistency mechanisms, especially where the GDPR leaves regulatory gaps.
12. The origin of a matter related to the interpretation of the GDPR could be a cross-border case as well as a national case, when the issue could also present itself in different Member States. The involved SAs may then decide to bring the matter before the EDPB in order to avoid setting a case law on their own on a sensitive subject.
13. In this context, it has to be underlined that such an opinion cannot be requested on the subject matter of a case but only on the underlying legal issues, which need to be solved in order to process the case on a factual level.

Example:

The Board could be requested to provide an opinion when a cross-border operating controller moves its main or single establishment to the territory of another Member State, resulting in questions regarding the competence of the former LSA and competence of the new LSA.

2.2.2 What is a “matter producing effects in more than one Member State”?

14. The second condition mentioned in Article 64 (2) GDPR refers to matters “producing effects in more than one Member State”. Firstly, this means that there must be effects in at least two Member States. These effects need to be factual in contrast to the definition of cross-border processing (Article 4 No. 23 GDPR), where the likelihood of effects is sufficient.
15. Secondly, given the fact that the wording of Article 64 (2) GDPR is not restricted to a special kind of effect, these effects must be understood as not being limited to legal effects. In contrast to the first condition which concerns abstract questions of a predominantly legal nature, this condition addresses effects of all kinds, for instance to the rights and freedoms of data subjects.
16. Article 64 (2) GDPR also serves as a tool to ensure consistency where no other instrument is applicable. This refers especially to questions arising from international cases where the One-stop-shop mechanism does not apply, but where a consistent approach is preferable.

Example 1: The processing activities of an US-based controller, without an EU establishment, produce effects in several EU Member States. When a question arises regarding one of the activities of this US-based controller, Article 64 (2) can be applied in order to ensure a consistent approach regarding this question.

Example 2: Another example of a practical application can be the situation where a LSA does not involve a SA in an Article 60 procedure although this SA is concerned according to Article 4 (22) and despite the SA informing the LSA about its status as a concerned SA.

2.2.3 Relationship between both conditions

17. It is likely that not all practical cases can be clearly allocated to one of these two conditions. A “matter of general application” can also be defined as a situation which produces legal effects with regard to categories of persons regarded generally and in the abstract. However, this first condition is formally unrelated to the second condition “producing effects in more than one Member State”, i.e. it is focused on the “generality” of the matter at issue. Nevertheless, there certainly are borderline cases where it is not feasible to draw a clear line between these two conditions.

2.2.4 Relationship to cooperation procedures (Article 60 et seq. GDPR)

18. As both conditions may arise from an ongoing individual case the relationship to cooperation mechanisms according to Article 60 et seq. GDPR has to be clear. First of all, it has to be noted though, that the primary objective with regard to cross-border cases is to reach consensus within the cooperation procedures (Article 60 et seq. GDPR) without involving the EDPB (Rec. 138 s. 2). Therefore, Article 64 (2) GDPR cannot be used to circumvent the cooperation mechanisms.
19. However, Article 64 (2) GDPR foresees the possibility to ask for an opinion of the EDPB “where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62”.
20. Articles 61 and 62 GDPR are tools which intend to achieve consistent and effective application of the GDPR. In cases where SAs refuse to comply with their duties to cooperate with other SAs via joint operations and mutual assistance Article 64 (2) GDPR serves as possibility to reach consistency by other means.
21. The following examples and counterexamples intend to clarify especially the relation between Article 60 et seq. and 64 GDPR, as requesting an opinion based on Article 64 (2) GDPR while a cooperation procedure is ongoing is the most complicated case of application. In this regard it should be noted that Article 60 (1) obliges the LSA and CSAs to cooperate with each other “in an endeavour to reach consensus”, which means that finding consensus without involving the Board is the preferable solution. This means that, as a best practice, informal cooperation procedures should be triggered before initiating formal procedures. Article 64(2) is the necessary tool if such consensus cannot be reached.

Example 1: A complex cross-border case is handled by the LSA, in good cooperation with two CSAs and in accordance with Article 60 GDPR. The case concerns, amongst others, a fundamental (new) legal question regarding the interpretation and application of Article 5 GDPR – purpose limitation. Taking into account the fundamental nature of the subject matter and the limited amount of SAs involved in the cross-border case the LSA and CSAs, in good cooperation and without there being any dispute on the question whether or not to request an opinion by the EDPB, may decide to request an Opinion of the EDPB, in order to achieve a consistent interpretation of the legal question at hand. This request

only covers the preliminary fundamental, underlying legal question regarding the interpretation and application of purpose limitation and not the ongoing cross-border case itself. The answer on the request is necessary for the involved SAs in order to be able to continue the drafting of a draft decision within the cooperation procedure.

Counterexample 1: A complex cross-border case is handled by the LSA. While cooperating with the two CSAs as set out in Article 60 GDPR, it becomes clear that one CSA does not agree with the approach of the LSA regarding the outcome of the case. The CSA does not want to wait for the draft decision of the LSA and considers invoking Article 64 (2) GDPR. In this case, Article 64 (2) GDPR should not be triggered, taking into account that both the LSA and CSAs need to follow the procedure as laid down in Article 60 GDPR. In practice this means that the LSA will submit a draft decision to the CSAs, while the CSAs have the opportunity to provide a relevant and reasoned objection should they disagree with this draft decision.

Example 2: The processing activities of a controller that concern personal data of a large number of data subjects in several EU Member States are – based on several complaints – subject to justified and substantial concerns of one or more CSAs. The LSA, however, after receiving the complaints does not inform the CSAs about the subsequent steps to handle the complaints or initiate an Article 60-procedure.

Taking into account that the CSAs that have received the complaints are obliged to inform the complainant about the state of play and the outcome of the complaint according to Article 77 (2) GDPR, requests for mutual assistance may be filed.

If the LSA does not comply with the obligations for mutual assistance in accordance with Article 61, the CSA may then request an opinion according to Article 64 (2).

Counterexample 2: On the other hand, there can be many valid causes for the extended duration of an investigation, particularly one with high stakes, with many of those reasons relating to fair procedures and the challenges in engaging with data controllers. In this case, Article 64 (2) GDPR cannot be triggered to request a LSA to accelerate the production of a draft decision when the investigation of a cross-border case is still ongoing, provided all requirements of Article 60 (1) or 61 are satisfied, in particular the exchange of all relevant information.

Example 3: Given that Article 60 GDPR is applicable, the situation might arise that the LSA does not provide a draft decision or any other outcome. In this situation, where informal requests for clarification and formal mutual assistance requests from the CSA according to Article 61 GDPR remained unsuccessful, the CSA may ultimately request an opinion on the LSA's non-compliance with the procedure of Article 61 GDPR.

Counterexample 3: However, Article 64 (2) GDPR cannot be triggered to request another SA to carry out a specific type of action or enforcement measure (according to Article 58 GDPR) regarding an ongoing cross-border case. The exercise of a corrective power must be subject to appropriate procedural safeguards and objective assessment. More importantly, there is no legal basis for the Board to compel specific measures based on Article 64 (2).

Example 4: The CSA sends a local case request to the LSA according to Article 56 (3) GDPR. The LSA does not reply within three weeks and the CSA's attempts to contact the LSA by other means such as

mutual assistance requests fail. The CSA may then, as a last resort, request the EDPB to obtain an opinion on the consequences of the absence of answer from the LSA.

Counterexample 4: Article 64 (2) GDPR may not be used to request another SA to prioritise specific cases provided that they respect the cooperation mechanism. Each SA is the only party with a full view of its own case load, the relative seriousness of those cases and the priorities that need to be applied.

2.3 ADMISSIBILITY REQUIREMENTS (ARTICLE 64 (2) GDPR)

22. The following admissibility requirements have to be met:

2.3.1 Possible applicants

23. The wording of the law is very clear on the question of who has the right to submit a request for an opinion under Article 64 (2) GDPR, namely any SA, the Chair of the Board or the Commission may request such an opinion. Other bodies, like e.g. data subjects are excluded from the possibility to submit such a request.

2.3.2 Substantive requirements

24. Furthermore, at least one of the two substantive requirements of Article 64 (2) GPDR has to be fulfilled. In practice, it may not be entirely clear which of the two conditions mentioned in Article 64 (2) GDPR is the most appropriate condition to base a request for an Opinion on. In these situations it is up to the requesting SA to decide whether it will base its request on one specific condition, or whether it will provide separate reasoning for both conditions. The SA can base its request either on one condition or on both conditions, which are laid down in Article 64 (2) GDPR. The decision on which condition to base the request, is at the discretion of the SA, whereas the Board makes the final decision. In this regard, it should be kept in mind that, in the end, it is the EDPB who decides whether or not a request will be rejected or not. If the conditions are not met the EDPB may reject the request on admissibility grounds.

2.3.3 Written reasoning

25. The applicant has to provide written reasoning (Article 10 (3) RoP) for the request. Doing otherwise would contradict Article 64 (4) GDPR, where reference is made to the need for the SA to provide the Board with any relevant information and documents. If the request is not reasoned, the EDPB can reject the request. In case the request is not sufficiently reasoned, the EDPB should - as best practice - ask for clarification if possible.

2.3.4 Exception from the right to obtain an opinion

26. Lastly, it is necessary that the EDPB has not already issued an opinion or decision in the sense of Article 65 (1) GDPR on the same matter before (Article 64 (3) s. 1 GDPR). If there are already similar opinions concerning similar matters the requesting SA, the Chair or the Commission has to provide reasoning why the request is not exactly on the same matter. This requires a prior assessment of the EDPB

opinions on similar matters. The EDPB may reject a request if there already is an opinion on that exact matter.

27. In all cases where the EDPB rejects a request for an opinion it is expected to indicate the reasons for rejecting the request on admissibility grounds (requirements a, b and c).

2.4 CONSEQUENCES

28. Article 65 (1) (c) GDPR states in its second alternative that in cases where a competent supervisory authority does not follow the opinion of the Board issued under Article 64, the Board shall, upon communication of the matter by any supervisory authority or the Commission, adopt a binding decision. As this alternative is not explicitly limited to either paragraph 1 or 2 of Article 64 GDPR, this must be applied to both situations where an opinion of the Board can be issued.
29. It follows from the above that in cases where, as a first step, the Board issues an opinion under paragraph 2 which is not followed by a supervisory authority, any supervisory authority or the Commission may communicate the matter to the Board again in order to obtain, as a second step, a binding decision pursuant to Article 65 (1) GDPR.

2.5 OUTLOOK

30. This guidance will be evaluated as deemed necessary with regards to practical experiences with Article 64 (2) taking into account especially the number and subjects of requests.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Internal EDPB Documents



Internal EDPB Document 4/2019 on the procedure for the adoption of the EDPB Opinions on the SA's draft accreditation requirements for certification bodies and the SA's draft decisions on criteria for certification

Adopted on 9 October 2019

IMPORTANT NOTE:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website. This document is currently being revised and some of the information in this document may no longer be up to date.

This document contains redactions as the publication of this information would undermine the decision-making process of the EDPB, in relation to matters upon which a decision has been taken.

Table of contents

1	EDPB OPINIONS ON SA'S DRAFT ACCREDITATION REQUIREMENTS FOR CERTIFICATION BODIES: SUBMISSION, ADMISSIBILITY AND OPINION	3
1.1	Preparation for submission of draft accreditation requirements to EDPB.....	3
1.2	Admissibility of draft accreditation requirements.....	4
1.3	Article 64 opinion.....	5
1.4	Further steps.....	5
2	EDPB OPINIONS ON SA'S DRAFT DECISIONS ON CRITERIA FOR CERTIFICATION (NATIONAL INITIATIVES): (INFORMAL REVIEW), SUBMISSION, ADMISSIBILITY AND OPINION	6
2.1	Preparation for submission of a draft decision to EDPB.....	6
2.2	Admissibility of a draft decision for criteria for certification.....	7
2.3	Article 64 opinion.....	8
2.4	Further steps.....	8

The European Data Protection Board

Having regard to Article 42(5), Article 43(3) and Article 64(1)(c) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

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

Having regard to Article 3 and Article 22 of its Rules of Procedure as last amended on 10 September 2019,

HAS ADOPTED THE FOLLOWING INTERNAL DOCUMENT

1 EDPB OPINIONS ON SA’S DRAFT ACCREDITATION REQUIREMENTS FOR CERTIFICATION BODIES: SUBMISSION, ADMISSIBILITY AND OPINION

1.1 Preparation for submission of draft accreditation requirements to EDPB

1. Supervisory authorities (SAs) have to draft and publish their requirements for accreditation of certification bodies pursuant to article 43.3. When they aim to approve these requirements, SAs have to submit them to the EDPB pursuant to article 64.1(c).
2. As agreed during the plenary meeting of April 2019, to better anticipate the workload of the EDPB, SAs should inform the other members in advance of their intention to submit a draft requirements for a consistency procedure. The Secretariat will share this information with the members of the Compliance, E Government Expert Sub Group (CEH ESG).
3. The formal submission has to be done via IMI platform. More information is available in the IMI user guide¹ and the IMI best practices².
4. It should be noted that, once a formal submission has been made, the decision will be prepared on the basis of the submitted documents, without a possibility for the CSA to update the submitted documents.

1.2 Admissibility of draft accreditation requirements

5. The submission shall fulfil the following admissibility criteria for acceptance by EDPB:
 - 1) All documents have to be submitted in English language;
 - 2) The EDPB assessment template is fully completed by the CSA and submitted;
 - 3) Relevant national legislation that has been referenced in the accreditation requirements; and
 - 4) A copy of the requirements for accreditation and any annexes are submitted.
6. The secretariat should check that all the documents are present and complete. The secretariat may request the CSA to provide the secretariat within a specific timeframe with additional information needed for the file to be complete. When necessary, for instance documents not originating or drafted by the supervisory authority, the documents submitted by the CSA will be translated into English by the secretariat without undue delay. When the CSA agrees on the translation, and the Chair and the CSA decide that the file is completed, the secretariat, on behalf of the Chair will circulate the file to the members of the Board.
7. The opinion of the Board shall be adopted within eight weeks after the Chair and the CSA (where relevant) have decided that the file is complete. It may be extended by a further six weeks, taking into account the complexity of the subject matter, upon decision of the Chair, on its own initiative or at the request of at least one third of the members of the Board.
8. Before draft opinions are submitted to the vote of the Board, they shall be prepared and drafted by the secretariat and, upon decision of the Chair, together with a rapporteur and expert subgroups members.
9. Upon decision of the chair, a drafting team can be set up, depending on the timing of submission, via email or at a CEH meeting. The call for the drafting team volunteers will be made by the Secretariat together with CEH experts group co-ordinators. In order to avoid conflicts of interest, the CSA should not be part of the core drafting team. However, any questions can always be addressed by the core drafting team to the CSA.
10. The CSA is called to take into consideration the working schedule of the CEH ESG before making its submission.
11. The Secretariat and the drafting team (where relevant) review the submitted requirements for accreditation and supporting documents (including the assessment template) and draft the opinion. This will always involve consideration of what was stated in previous opinions on the same subject, in order to ensure consistency. The EDPB assessment template submitted by the CSA can be used as an internal working document when preparing the draft opinion. This review must take place within the opinion deadlines.

1.3 Article 64 opinion

12. Under article 64, EDPB shall issue an opinion pertaining to matters outlined in article 43(3) of the GDPR.
13. The rules of article 10 of the EDPB rules of procedure apply for the adoption of an opinion.

1.4 Further steps

14. The following steps have to be fulfilled after the adoption of an opinion:
 - (1) the Secretariat publishes the opinion;
 - (2) Within two weeks of receipt of the Opinion, the SA shall communicate to the Chair its intention to maintain or amend the decision and the amended draft decision, if any. The answer will be analysed by the SEC, the rapporteurs and the ESG members who prepared the opinion, in line with Art. 10.7 of the EDPB's RoP. The SEC will circulate this information to the members of the Board;
 - (3) the CSA adopts its draft decision, making its accreditation requirements public.

2 EDPB OPINIONS ON SA'S DRAFT DECISIONS ON CRITERIA FOR CERTIFICATION (NATIONAL INITIATIVES): (INFORMAL REVIEW), SUBMISSION, ADMISSIBILITY AND OPINION

2.1 Preparation for submission of a draft decision to EDPB

16. Scheme owners (which could be organisations or private companies that are not in charge of issuing certificates) or certification bodies should formally submit their certification criteria to their local SA. Furthermore, SAs can also draft the criteria for certification of a certification mechanism, act as a certification body and perform accreditation itself.³
17. SAs have the power to approve criteria for national certification schemes referred to in article 42(5) and article 58(3)(f). The SA shall carry out a review to ensure that draft certification criteria meet the requirements of a GDPR certification scheme, taking into account the EDPB guidelines on certification. The SA's review will be aided by fully completing the assessment template sections for national criteria. When it aims to approve these criteria, the SA has to submit their draft decision to the EDPB pursuant to article 64.1(c).
18. Where there is consideration of approval of criteria by multiple SAs, depending on the stage of submission and approval, it may be possible to streamline the opinion route⁴. For example:
 - 1) if the CSA considers that draft criteria for certification in its submission have already been subject to an EDPB opinion, it should highlight this with appropriate references;
 - 2) if the CSA considers that draft criteria for certification in its submission are an amended version of criteria that have already been subject to an EDPB opinion (e.g. to take into account national law), the CSA should highlight the amended elements in its submission and provide a reasoning of the potential impacts of the changes overall the set of the certification criteria.
19. The formal submission has to be done via IMI platform. More information is available in the IMI user guide and the IMI best practices (refer to ²).
20. The submission for informal review is done using the EDPB digital shared workspace tool.
21. Before formally submitting its draft decision, the CSA can decide whether the submission would be assisted by an informal review. Pursuant to article 57.1(g), the CSA should "*cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of*" the GDPR.

³ A CSA cannot submit certification criteria for an opinion if it has not already submitted the CSA's accreditation requirements for approval.

⁴ As specified in the EDPB guidelines, CSA are called to avoid fragmentation of the data protection certification market

22. This informal phase allows the CSA to get early feedback and seek further information from the scheme owner, before submitting a draft decision for an EDPB opinion⁵. Regardless of the review route chosen by the CSA, it should be noted that, once the formal submission is made, the decision will be prepared on the basis of the submitted documents, without a possibility for the CSA to update the submitted documents. Please see the work flow chart below for more information about the stages in this process.

2.2 Admissibility of a draft decision for criteria for certification

23. The submission (for both formal and informal routes) shall fulfil the following admissibility criteria for acceptance by EDPB:
- All documents have to be submitted in English language; and
 - The EDPB assessment template is fully completed by the CSA and submitted; and
 - A copy of the criteria for certification and any annexes are submitted.
24. The secretariat will check that all the documents are present and complete. The secretariat may request the CSA to provide the secretariat, within a specific timeframe, with additional information needed for the file to be complete. When necessary, for instance documents not originating or drafted by the supervisory authority, the documents submitted by the competent authority will be translated into English by the secretariat without undue delay. When the competent authority agrees on the translation, and the Chair and the CSA decide that the file is completed, the secretariat, on behalf of the Chair, will circulate the file to the members of the Board.
25. The opinion of the Board shall be adopted within eight weeks after the Chair and the CSA (where relevant) have decided that the file is complete. It may be extended by a further six weeks, taking into account the complexity of the subject matter, upon decision of the Chair on its own initiative or at the request of at least one third of the members of the Board.
26. Before draft opinions are submitted to the vote of the Board, they shall be prepared and drafted by the secretariat and, upon decision of the Chair, together with a rapporteur and expert subgroups members. Depending on the scope of the certification mechanism, expertise of other EDPB subgroups may be requested in order to prepare the opinions.
27. Upon decision of the chair, a drafting team can be set up, depending on the timing of submission, via email or at a CEH meeting. The call for the drafting team volunteers will be made by the Secretariat together with CEH experts group co-ordinators. In order to avoid conflicts of interest, the CSA should not be part of the core drafting team. However, any questions can always be addressed by the core drafting team to the CSA.

⁵ The formal review phase without the informal review phase would normally only be possible when the CSA has already held extensive consultations and be able to demonstrate these and satisfactorily explain why the informal review phase is not required.

28. The CSA is called to take into consideration the working schedule of the CEH experts group before making its submission.
29. The secretariat and the drafting team (where relevant) review the submitted criteria for certification and supporting documents (including the assessment template) and draft the opinion. This will always involve consideration of what was stated in previous opinions on the same subject, in order to ensure consistency. The EDPB assessment template submitted by the CSA can be used as an internal working document when preparing the draft opinion. This review must take place within the opinion deadlines.

2.3 Article 64 opinion

30. Under article 64, EDPB shall issue an opinion pertaining to matters outlined in Article 42(5) of the GDPR.
31. The rules of article 10 of the EDPB rules of procedure apply for the adoption of an opinion.

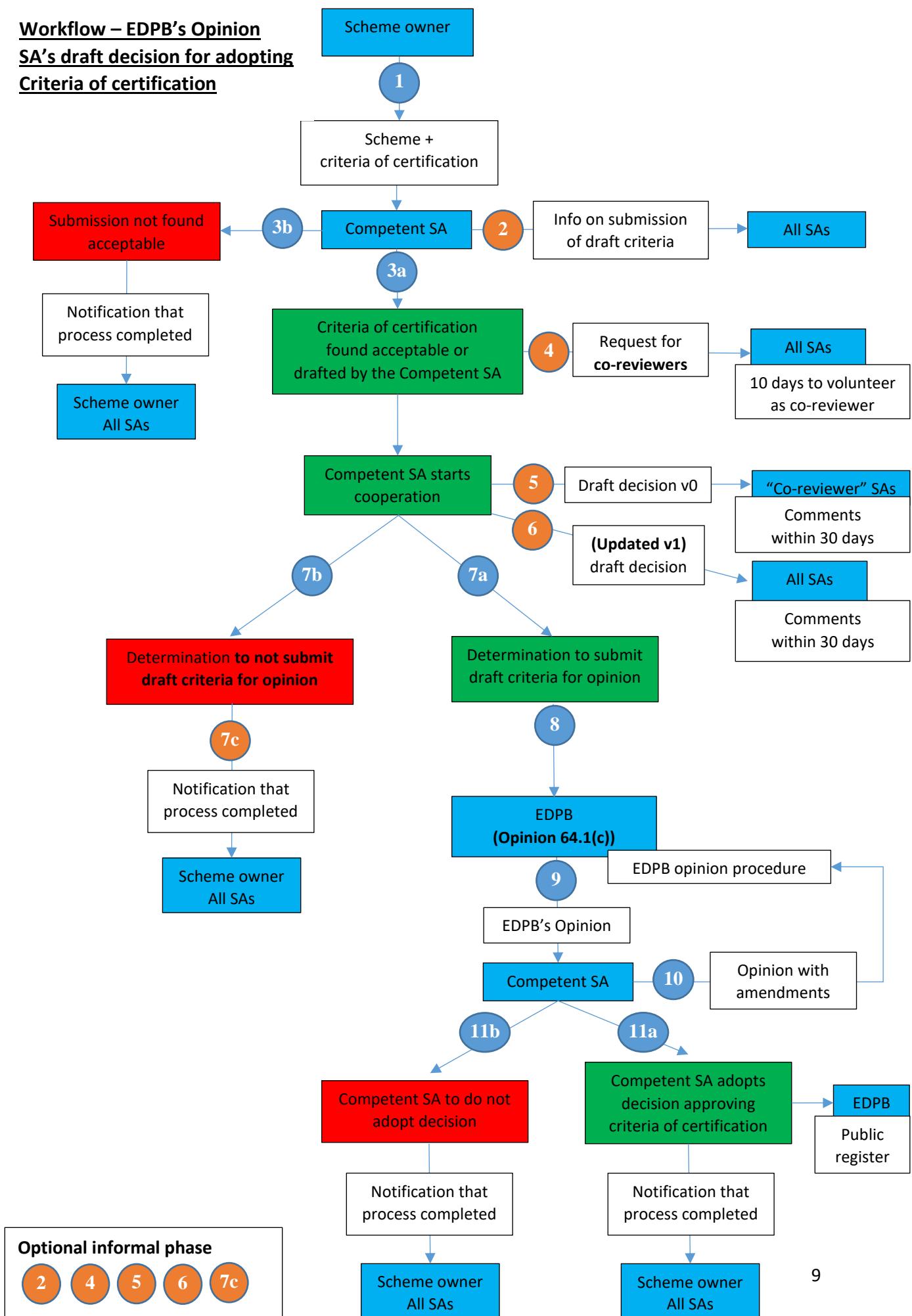
2.4 Further steps

32. The following steps have to be fulfilled after the adoption of an opinion:
 - (1) the Secretariat publishes the opinion;
 - (2) Within two weeks of receipt of the Opinion the SA shall communicate to the Chair its intention to maintain or amend the decision and the amended draft decision, if any. The answer will be analysed by the SEC, the rapporteurs and the ESG members who prepared the opinion, in line with Art. 10.7 of the EDPB RoP. The SEC will circulate this information to the members of the Board;
 - (3) the CSA adopts its draft decision, making it public.
 - (4) the CSA should inform the scheme owner about the adoption of the draft decision in relation with the EDPB's opinion;
 - (5) the CSA is responsible for ensuring the transmission to the Secretariat of the required documents for the publication in the EDPB public register.

Workflow – EDPB's Opinion

SA's draft decision for adopting

Criteria of certification



Internal EDPB Documents



Internal EDPB Document 04/2021 on criteria of territorial competence of supervisory authorities to enforce Article 5(3) of the ePrivacy Directive

Adopted on 18 June 2021

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

The European Data Protection Board

HAS ADOPTED THE FOLLOWING INTERNAL DOCUMENT

1 BACKGROUND

1. A number of recent decisions adopted by some supervisory authorities (“SAs”) competent for the enforcement of Article 5(3) of the ePrivacy Directive¹ show that the territorial application of this directive may differ across SAs, in particular when a controller / service provider has establishments in several member states.
2. The aim of this document is to establish a common interpretation of the territorial competence of SAs responsible for enforcing Article 5(3) of the ePrivacy Directive, whatever the choices made by each Member State when transposing the ePrivacy Directive. This point is not specifically covered in the Opinion on the Interplay between the ePrivacy Directive and GDPR². However, uncertainty on such a fundamental question would risk jeopardizing decisions adopted by the SAs across the European Union.

2 DISCUSSION

3. Article 17(1) of the ePrivacy Directive provides that “*Member States shall bring into force the provisions necessary to comply with this Directive*” and Article 15(1) provides that “*Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented*”. It follows from these provisions that it is thus up to each Member State to take the necessary measures to ensure that the objectives set by the ePrivacy Directive are achieved.
4. However, the ePrivacy Directive remains silent regarding its territorial application. Consequently, the case-law of the CJEU on the territorial application of the repealed directive 95/46/EC gives an indication of how the territorial application should be organised. Indeed, in the case *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, 5 June 2018, the Court stated that the supervisory authority of a Member State was entitled to exercise its powers against an establishment of an undertaking situated in its territory and in the course of whose activities the processing is carried out, even if the establishment responsible for the collection and processing of data was situated in another Member State³.

¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC.

² 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.

³ The Court ruled that “*Articles 4 and 28 of Directive 95/46 must be interpreted as meaning that, where an undertaking established outside the European Union has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State.*”

5. If the data controller/service provider has no establishment in a Member State, the national law of this Member State may provide other criteria than establishment to enforce its national law in respect of this controller/service provider.
6. It stems from these elements that each competent SA is entitled to enforce its national law transposing the ePrivacy Directive, as far as it concerns users located in its territorial jurisdiction. It also implies that no legislation transposing the ePrivacy Directive may prevent the SA of another Member State to enforce the ePrivacy Directive in accordance with its national provision, with respect to users located in its territorial jurisdiction⁴. Otherwise, this would not be consistent with the objective of protecting the fundamental rights and freedoms of data subjects, as set by Article 1(1) of the ePrivacy Directive.
7. Ultimately, it would mean that the fine imposed on a controller/service provider would depend on the national legislation of one single Member State. Considering that maximum sanctions for an infringement of the ePrivacy Directive vary significantly across Member States (with some legislations providing for smaller fines), it would mean that, in certain cases, fines might not be a deterrent ensuring an effective protection of European users' data and this could reactivate, at the same time, a risk of forum shopping⁵.
8. This does not prevent the SAs to initiate a spontaneous cross border dialogue with the objective to create harmonised conditions regarding ePrivacy matters, as provided by Article 15a (4) of the ePrivacy Directive.

3 CONCLUSION

9. **Consequently, when the processing is regulated exclusively by the national law provisions transposing Article 5(3) of the ePrivacy Directive, the EDPB considers that SAs competent for the enforcement of Article 5(3) of the ePrivacy Directive are entitled to exercise the powers conferred on them by their national law, whenever:**
 - **the controller/service provider is established in their territorial jurisdiction;**

It should be noted that in the case at stake, the processing in question was carried out "in the context of the activities" of the establishment in question.

⁴ In its opinion in the case *Wirtschaftsakademie Schleswig-Holstein*, the Advocate General stated:

"95. *The fact that, by contrast with the situation in the case which gave rise to the judgment of 13 May 2014, Google Spain and Google, (56) the Facebook group has a European head office, in Ireland, does not mean that the interpretation of Article 4(1)(a) of Directive 95/46 which the Court adopted in that judgment cannot be applied in the present case. In that judgment, the Court voiced the intention that the processing of personal data should not escape the obligations and guarantees laid down by Directive 95/46. It has been suggested in the present proceedings that the problem of such circumvention does not arise here, because the controller is established in a Member State, namely Ireland. According to that logic, Article 4(1)(a) of Directive 95/46 should be interpreted as requiring that controller to have regard to the legislation of only one Member State and to answer to only one supervisory authority, that is to say, Irish legislation and the Irish authority. Such an interpretation, however, is contrary to the wording of Article 4(1)(a) of Directive 95/46 as well as to the origins of that provision.*

96. Such an interpretation, however, is contrary to the wording of Article 4(1)(a) of Directive 95/46 as well as to the origins of that provision. Indeed, as the Belgian Government rightly observed at the hearing, the directive does not introduce a one-stop-shop mechanism or a country-of-origin principle [...] The result, arrived at in Directive 95/46, reflects the wishes of the Member States to preserve their national powers of enforcement. By not adopting the country-of-origin principle, the EU legislature enabled each Member State to apply its own national legislation and thus made the application of multiple national legislations possible.

⁵ Article 15 a (1) of the ePrivacy Directive states "The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified."

- the processing is carried out in the context of the activities of an establishment located in their territorial jurisdiction, even when exclusive responsibility for collecting and processing belongs, for the entire territory of the European Union, to an establishment situated in another Member State;
- in the absence of controller/service provider or establishment in their territorial jurisdiction, the national law provides another criterion for its enforcement.

10. In any event, the measures taken:

- should not concern users located in a territorial jurisdiction for which the SA is not competent;
- should not prevent another competent SA to enforce the ePrivacy Directive in respect of its territorial jurisdiction.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Internal EDPB Documents



**Internal EDPB Document 5/2021 on handling complaints against public authorities or private bodies acting on the basis of Article 6(1), point (c) or (e),
GDPR in another EEA Member State**

Adopted on 07 July 2021

Important note:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of contents

1. Scope	3
2. Background	3
3. Practical Guidance	4
3.1 SA RECEIVING A PUBLIC SECTOR COMPLAINT FOR WHICH IT IS NOT COMPETENT UNDER 55.2 GDPR.....	4
3.2 SA HANDLING A PUBLIC SECTOR COMPLAINT FOR WHICH IT IS COMPETENT UNDER 55.2 GDPR	5
ATTACHMENT	7

The European Data Protection Board

HAS ADOPTED THE FOLLOWING INTERNAL DOCUMENT

1. Scope

1. This internal guidance document is meant to address the handling of those cases where a complaint is received by an EEA SA (the ‘complaint-receiving SA’) concerning processing activities by a public authority (or a private body acting under 6(1)c or 6(1)e) GDPR in a different EEA MS, in order to outline shared cooperation approaches that can be relied upon by SAs.

2. Background

2. In these cases the SA of the MS where the public authority operates is exclusively competent under Article 55(2) GDPR (the ‘competent SA’). However, all EEA SAs are required to cooperate under 57(1)g GDPR to ensure consistency of application and enforcement of the GDPR - therefore, including cases regarding public bodies or authorities.
3. Article 61(1) GDPR provides for mutual assistance obligations between EEA SAs ‘in order to implement and apply this Regulation in a consistent manner’; this wording implies that mutual assistance is an overarching obligation, i.e. regardless of whether assistance is sought as part of OSS procedures or not. Accordingly, SAs ‘shall put in place measures for effective cooperation with one another’.
4. Moreover, Article 77(1) GDPR allows data subjects to lodge complaints with ‘a’ supervisory authority – which may be ‘in particular’ the one in the MS ‘of his or her habitual residence, place of work or place of the alleged infringement’. Accordingly, it can be argued that a data subject is entitled to lodge complaints with the SA that is closest to their centre of interests even though that SA is not competent for handling the complaint under Article 55(2) GDPR. Data subjects are not required to address themselves to the SA that is competent under the GDPR as it will rather be up to the SAs to sort out this competence between them in accordance with the GDPR.
5. It should also be recalled in this respect that Article 77(2) GDPR requires the complaint-receiving SA to inform the complainant on progress and outcome of the complaint. This may have relevance as regards the need for all EEA SAs as administrative bodies to ensure effectiveness and efficiency of their administrative action pursuant to general principles of EU law (Article 41 CFR, in particular, as applied jointly with Article 51 CFR) and national law – in that the most efficient way should be determined to inform the complainant pursuant to Article 77(2) including when such complainant is habitually resident in a different EEA MS.

6. Taking account of the above considerations, it appears to be necessary to clarify how EEA SAs may cooperate in practice to handle complaints addressed against public bodies or authorities in a different MS so as to ensure a consistent application of the GDPR also in such cases and fully uphold data subjects' rights whilst avoiding procedural pitfalls.
7. On the one hand, there is indeed a risk that a data subject may experience difficulties in staying abreast of the complaint-handling proceeding in the competent SA's MS on account of possible language and legal barriers, so that it is imperative that his or her right to be informed on the progress (and outcome) of the complaint pursuant to Article 77(2) GDPR is upheld to the maximum possible extent. This is a difficulty that does not arise in the context of an OSS proceeding, where the CSA remains a party to the proceeding throughout its development and acts as the one-stop-shop for the complainant (the key interlocutor for the complainant).
8. On the other hand, there is the risk that the proceeding before the competent SA may be marred by the activities of the complaint-receiving SA insofar as such activities may conflict with the exclusive competence recognised in such cases to only one SA under Article 55(2) GDPR. It should be avoided that the complaint-receiving SA undertakes activities or takes initiatives that are not based on specific requests by the competent SA and thus becomes ultimately liable for those activities and initiatives especially in the complainant's eyes.

3. Practical Guidance

9. For the purposes of this document, a distinction can be drawn by considering the role of the complaint-receiving SA and that of the competent SA separately.

3.1 SA RECEIVING A PUBLIC SECTOR COMPLAINT FOR WHICH IT IS NOT COMPETENT UNDER 55.2 GDPR

PROPOSED BEST PRACTICES

10. The complaint-receiving SA will inform the complainant that it is not competent to carry on the proceeding under Article 55(2) GDPR and that he/she will have to interact directly with the competent SA regarding the complaint, but that it will forward the complaint (as is) to the competent SA if the complainant agrees to it, where applicable under national law. It will provide the complainant with the contact details of the competent SA, if possible including the relevant department/unit.
11. The complaint-receiving SA will immediately inform the competent SA that it received the complaint using IMI Art 61 VMA¹. By the same means, with the complainant's agreement where this is applicable under national law, it will forward the complaint (as is) along with

¹ It should be recalled that it has already been agreed (see Article 56.2 internal guidance) that a SA that is not competent to handle the given case/complaint may use the Art. 61 Voluntary Mutual Assistance procedure to pass on the case/complaint to the competent SA.

- (at least) a summary of the complaint in English for the sake of cooperation under Art. 57(1)g GDPR.
12. The complaint-receiving SA will remain available for further interactions with the competent SA, upon the latter's request, and with the complainant, in pursuance of Article 77(2). Further procedural steps concerning the complaint-receiving SA (e.g.: closing the procedure) will be regulated in accordance with the complaint-receiving SA's national law.
 13. A **template information sheet/letter** is provided as an attachment to this document; it may be used on a voluntary basis by the complaint-receiving SA to convey the necessary information to the complainant.

3.2 SA HANDLING A PUBLIC SECTOR COMPLAINT FOR WHICH IT IS COMPETENT UNDER 55.2 GDPR

PROPOSED BEST PRACTICES

14. The competent SA under Article 55(2) will confirm reception of the submission as forwarded by the complaint-receiving SA via IMI Article 61 VMA along with a short English summary.
15. The competent SA will perform a preliminary vetting of the submission based on the English summary, in order to assess at least admissibility under the national law. It will inform the complainant (either directly or via the complaint-receiving SA using an Article 61 VMA request) about the subsequent steps also regarding admissibility of the complaint.
16. In particular, the complainant will be informed as soon as possible whether he/she will have to lodge the complaint directly with the competent SA, in a language that is admissible under the competent SA's national law, to meet national law requirements.
17. Due to the lack of competence of the complaint-receiving SA, the latter is barred in principle from handling the complaint directly. However, the two SAs may determine further cooperation activities, on a voluntary basis, as appropriate to the case at hand. It will be for the competent SA to determine such activities in accordance with the competent SA's national law and in the light of Article 61 GDPR. The complaint-receiving SA may act as a facilitator or intermediary mainly with respect to the competent SA's contacts with the complainant.
18. For the purpose of informing the complainant about the progress of the complaint pursuant to Article 77(2) GDPR, the competent SA may also rely on the complaint-receiving SA's assistance using an Article 61 VMA request.
19. There may be cases where the objective of Article 77(2) GDPR and the rationale of Recital 129 GDPR may be better fulfilled by involving the complaint-receiving SA in the exchanges with the complainant (e.g. in terms of language barriers and the exercise of the complainant's right to be heard) - although it may be argued that the legal framework in the competent SA's MS already takes care of such situations and enables hearing the complainant without 'superfluous costs and excessive inconveniences' as mentioned in Recital 129 GDPR. As pointed out above, this may only take place on the basis of a request

made by the competent SA to the complaint-receiving SA and by taking account of the constraints of the competent SA's national law.

20. Based on the experience gathered in this area, it will be considered whether further best practices need to be defined in order to streamline the information flow between the complaint-receiving SA and the competent SA, in any case based on the impulse and input provided by the latter.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

ATTACHMENT

TEMPLATE INFORMATION LETTER FOR COMPLAINANT

(suggested for use by the complaint-receiving SA, if appropriate)

Dear Madam/Sir,

We are writing further to your complaint as lodged with our SA on ... regarding [brief description of complaint] [national reference No ...].

We would like to inform you that our SA is not competent to handle your complaint, as it is addressed against [select appropriate option] a public body/a public authority/a private body acting in compliance with a legal obligation under the law of/ for the performance of a task carried out in the public interest of/ [name of MS]. Under Article 55(2) of the GDPR, in such cases the SA of the MS concerned is competent; accordingly, you should contact: [name of competent SA and contact details].

[Select appropriate wording] Please consider that our SA can forward your complaint to the [competent SA] if you agree to it; in that case, please let us know at your earliest convenience as we will also provide the [competent SA] with a short English summary of your complaint. If we do not hear from you by [deadline], we will consider that you do not intend us to proceed in this manner. // We would also like to inform you that we will forward your complaint to the competent SA jointly with a short English summary.

Please consider that you may be contacted by the [competent SA] requesting you to lodge your complaint with it in accordance with its national law requirements. In any case, all future contacts regarding your complaint will be handled by the [competent SA].

For your information, our SA may provide the [competent SA] with assistance in handling your complaint if requested to do so, including in order to inform you about the progress of the complaint.

Yours Sincerely,

Letters



Ms Mairead McGuinness
European Commissioner for Financial services,
financial stability and Capital Markets Union

Mr Didier Reynders
European Commissioner for Justice
by e-mail only

Brussels, 19 May 2021

Ref: OUT2021-0088

Dear Commissioner McGuinness,
Dear Commissioner Reynders,

This letter follows the adoption by the EDPB, on 15 December 2020, of a Statement on the protection of personal data processed in relation with the prevention of the use of the financial system for the purposes of money laundering and terrorist financing¹, as well the adoption by the European Commission of an Action Plan² for a comprehensive Union policy on preventing money laundering and terrorist financing and the launch of a public consultation³ in May 2020.

The Commission aims to present new legislative proposals in 2021, *inter alia*, establishing a single rulebook on these topics (i.e. a Regulation or a more detailed revised Directive), ensuring EU level supervision (either by granting new powers to an existing EU Agency or by establishing a new dedicated body), and creating a support and coordination mechanism for Financial Intelligence Units.

The core purpose and function of the AML Directives and their subsequent transposition into EU member state domestic laws are for.... "*the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*". It is important to keep this statement in mind when considering the data protection implications of AML laws, because the key method for monitoring AML is to follow the monetary transactions in order to detect suspicious money flows.

¹ Statement on the protection of personal data processed in relation with the prevention of the use of the financial system for the purposes of money laundering and terrorist financing, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_amlactionplan_en.pdf.

² Action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 7 May 2020, available at https://ec.europa.eu/info/publications/200507-anti-money-laundering-terrorism-financing-action-plan_en.

³ The consultation can be accessed at: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12176-Action-Plan-on-anti-money-laundering/public-consultation>.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Considering that the EDPB, and before it the Article 29 Working Party, has repeatedly noted the privacy and data protection challenges related to the AML-CFT framework⁴, the EDPB wish to advise the Commission on this subject matter before the presentation of the legislative proposals, pursuant to Article 70 GDPR. Indeed, a fair balance has to be struck between the interest to prevent money laundering and terrorist financing, on the one hand, and the interests underlying the fundamental rights to data protection and privacy, on the other.

Furthermore, the EDPB recommends the Commission to include specific provisions in the upcoming legislative proposals in order to specify the application of the GDPR in the context of the AML-CFT legal framework, pursuant to Article 6 (3) of the GDPR. The EDPB notes that the current AML-CFT legislation already contains a provision on the purpose limitation principle⁵, which effectiveness is crucial and should be carefully assessed by authorities. To promote compliance and create more legal certainty for obliged entities, the EDPB recommends that the new AML-CFT instruments contain specific provisions with regard to the general conditions governing the lawfulness of processing by obliged entities and the personal data that is provided by third parties (see section 3 below); the types of data which are subject to the processing of personal data in the context of AML-CFT obligations; the data subjects concerned; the entities to, and the purposes for which the personal data may be disclosed; the specifications of storage periods, and processing operations and processing procedures, including measures to ensure lawful and fair processing.

Moreover, the EDPB recommends the inclusion in the legislative proposals of appropriate safeguards to ensure the respect of the data protection by design and by default obligations in the AML-CFT framework pursuant to Article 25 GDPR, including through techniques such as data avoidance (i.e. to avoid processing personal data altogether when this is possible for the relevant purpose), separation (i.e. to separate the processing of personal data as much as possible), abstraction (i.e. to limit as much as possible the detail in which personal data are processed) and security measures such as access restriction, obfuscation (i.e. to make data incomprehensible), encryption or dissociation of personal data (i.e. to break the link and the correlation between events, persons and data)⁶.

Additionally, the EDPB recalls that the following personal data protection principles are of utmost, and equal, importance in the AML-CFT context. They should be taken into account, at each stage, to ensure that the anti-money laundering measures are compatible with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

1. Proportionality and efficient risk-based approach

⁴ See for instance Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf.

⁵ See Article 41(2) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

⁶ See EDPB Guidelines4/2019 on Article 25 Data Protection by Design and by Default, available at : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf. See also Jaap-Henk Hoepman, *Privacy design strategies*, January 27, 2020. [pdfs-booklet.pdf \(ru.nl\)](#)

The EDPB recalls that, pursuant to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union as interpreted by the case law of the European Union, the AML-CFT framework shall respect the principles of necessity and proportionality. It implies that different cases should be treated differently, proportionately to their relevant differences.

Pursuant to Article 52 of the Charter, any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others⁷. This means that legislative measures that limit the right to privacy and data protection have to be specific in order to correspond to objectives of general interest pursued and should not constitute disproportionate and unreasonable interference undermining the substance of those rights.⁸

The EDPB highlights that the GDPR is the general data protection framework, and does not contain sector specific data protection rules; therefore, for specific areas, it is important that the legislator lays down these specific data protection rules in the law in accordance with Article 6(3) of the GDPR.

Under the AML-CFT legislation, obliged entities must identify and report suspicious transactions, that is, the situations where the financial system could be used to launder the proceeds of crimes or to fund terrorist activity. This has proven difficult to do, as the standard for ensuring that the transaction is legitimate is based on a reasonable risk-based approach⁹, which is a standard that is not clearly enough quantified or defined in legislation or through guidance from regulatory bodies. Consequently, the monitoring of financial transactions produces a large quantity of false positive alarms, where the transaction is not associated with money laundering or terrorist financing and therefore it is not reported to the FIU.

The Board therefore recommends that the specifics as to what the obliged entities should be monitoring should be clearly defined and guidance provided as to what exactly is required from a reasonable risk-based approach.

Furthermore, the EDPB recommends that the trigger events as to when further investigation should occur, should be distinct and clear so as, to avoid any disproportionate and therefore unlawful processing of personal data of any individual.

Moreover, the processing operations carried out by the AML officers of obliged entities, when suspicious financial or monetary transactions are detected and require further investigation as to the individuals concerned, should be accompanied by rigorous safeguards from a data protection perspective. It is important to state that it should not be a "*one size fits all*" approach as the scrutiny of an individual's financial movements should only really happen where there is suspicious transactions or activity occurring. Otherwise, if such close individual scrutiny occurred on all

⁷ See also Article 23 GDPR and the EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR.

⁸ See ECJ judgement of 13 April 2000, Case C-292/87, para. 45.

⁹ See Article 18(2) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

individuals in the customer databases of obliged entities, there could be unnecessary and disproportionate processing of their personal data and probably not proportionate under data protection laws and possibly ultra vires to the legal requirements under AML-CFT.

Moreover, concerning Enhanced Due Diligence (EDD), it is important that obliged entities establish clear and transparent criteria of the individuals falling into such category. Indeed, the EDD involves inter alia, the request and review by the obliged entity of extensive information about the individual falling within this process, as well as multiple person access to the data (i.e. before establishing a business relationship, approval from the obliged entity's senior manager is required in line with Article 19 of the AML D4). The Board therefore recommends that the parameters as to when EDD occurs are strict so as to avoid disproportionate and therefore excessive processing of personal data.

2. Data minimisation

Pursuant to the data minimization principle provided by Article 5(1) (c) of the GDPR, obliged entities must process only the personal data that are necessary to comply with the AML-CFT framework.

The EDPB therefore recommends that the AML-CFT legislation specify what is necessary and proportionate to comply with its obligations. From a data protection perspective, it is crucial to insert language in every AML obligation that clarifies whether the personal data necessary to comply with a specific obligation should (only) be collected from the data subject or whether other sources (e.g. third party) can/must be used (public / non-public). It is also necessary to specify whether or not and, if yes, which types of special categories of personal data and/or personal data relating to criminal convictions and offences can/must be processed to comply with that specific obligation.

Additionally, defensive behaviour of obliged entities – which leads them to send large quantities of non-material suspicions, generating a high number of false positive reports – should be avoided. The EDPB recommends that the new AML-CFT legislation explicitly contain requirements that only accurate and relevant data can be used for reports. These requirements should also specifically prohibit the inclusion of personal data relating to criminal convictions and offenses that are not connected to AML-CFT.

3. Data accuracy

The accuracy and reliability of data is an important aspect, not only from a data protection perspective as enshrined in Article 5(1) (d) of the GDPR, but also for the effectiveness of AML-CFT obligations. Therefore, the EDPB recommends that the AML-CFT legislation states that personal data processed by obliged entities shall be accurate, reliable, and up to date in order to comply with the AML-CFT obligations.

The EDPB observes that the applicable AML-CFT measures include very broad and 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 transactions¹⁰.

The Board therefore recommends to include a legal obligation in the coming legislative proposals for obliged entities to implement appropriate data protection policies with regard to the processing of personal data for AML-CFT purposes, within the meaning of Article 24(2) of the GDPR, as this would be appropriate and proportionate in relation to the processing activities that take place in this context, considering their nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The Board also recommends to specify that these policies shall include the collection of personal data from third parties whose services are used or the processing by third parties to whom certain processing activities are outsourced.

More specifically, obliged entities are increasingly dependent on external sources known as “watchlists”, which are provided by third parties. These “watchlists” are commonly used by obliged entities to screen their databases and verify relevant information about their clients, in order to fulfil their legal obligations, and notably to assess the risk of the business relationship. The providers of these “watchlists” are in general controllers under the GDPR and do not fall under the current AML-CFT legislation. Nevertheless, the data processing performed in the context of these watchlists raise serious concerns, considering the quantity and sensitive nature of personal data they process which could lead to serious damage to the rights and freedoms of data subjects. Moreover, the fact that obliged entities make use of these databases provided by third parties does not exempt them from ensuring the accuracy of personal data that they process.

The EDPB therefore recommends to seize to create a specific legal framework for “watchlists” and, in particular, to clarify the responsibilities between obliged entities and the watchlists providers regarding GDPR obligations, to provide guarantees especially regarding the compilation of sensitive data, as well as to regulate the consultation of those lists by obliged entities and specify how data subject rights are respected in this context. .

4. Storage limitation

Pursuant to Article 5(1) (e) of the GDPR, all personal data processed for AML-CFT purposes must not be retained unnecessarily and indiscriminately. The EDPB therefore recommends that the AML-CFT legislation specify which personal data has to be retained and for how long, taking into account the necessity¹¹ and proportionality¹² principles. For instance, a distinction in the applicable storage period could be made between, on the one hand, data related to executed or intended transactions which

¹⁰ See Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing, adopted on 15/12/2020, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_amlactionplan_en.pdf.

¹¹ See EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017.

¹² See EDPS, Assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019

Andrea Jelinek

Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

have been deemed suspicious and reported to the financial intelligence unit and, on the other hand, data related to unsuspicious transactions.

5. Processing of special categories of personal data and processing of personal data relating to criminal convictions and offences

Processing of special categories of personal data, within the meaning of Article 9 of the GDPR, and processing of personal data relating to criminal convictions and offenses, are prohibited except if one of the exceptions provided by the GDPR applies, or, in the case of personal data regarding criminal convictions and offences, the processing shall be laid down in specific legal provisions. In the AML-CFT context, the only applicable derogation to the processing of special categories of personal data is the one provided by Article 9(2) (g) of the GDPR, which allows such processing if it is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Similarly, Article 10 of the GDPR required that processing of personal data relating to criminal conviction and offences by obliged entities should be authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects

The EDPB noticed that there are currently wide differences between Member States laws regarding the provision of such derogations and safeguards. Therefore, the EDPB considers that there is a need for harmonization to enhance both the legal certainty and the EU citizens' right to data protection.

In addition, according to Articles 9(2) (g) any law allowing the processing of the special categories of personal data shall contain suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. According to Article 10 of the GDPR, personal data regarding criminal convictions and offenses, shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Therefore, the GDPR requires that the legislator specifies the general data protection principles of the GDPR into these new AML-CFT instruments. Indeed, appropriate and specific safeguards are necessary to comply with the GPDR. For instance, regarding the processing of personal data relating to criminal convictions and offenses, it could be provided that obliged entities should only be allowed to process criminal convictions and offences related to money laundering and terrorist financing handed down in countries where the rule of law, and especially the presumption of innocence, the right of defence and right of a fair trial are respected. Another appropriate safeguard could be to ensure the training and expertise of staff that deal with sensitive personal data in the context of AML-CFT obligations. All safeguards should be accompanied by serious corrective measures, including penalties, for the controller (obliged entity or FIU as the case may be) in case of non-compliance.

6. Independent supervisory authorities

To ensure the application of the data protection principles in the AML-CFT context, a cooperation between AML-CFT supervisory authorities and data protection authorities should be laid down in the texts. The EDPB therefore recommends to specify in the AML-CFT framework that the European Commission and the European supervisory authorities should consult the EDPB prior enacting

Andrea Jelinek

Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

delegated act, guidelines or recommendations involving additional processing of personal data or affecting the right to data protection. Similarly, in those cases, the Member States AML-CFT competent authorities should consult the national data protection authorities.

Conclusion

To conclude, the EDPB urges the European Commission to propose specific provisions in the future AML-CFT legal framework in order to adapt the application of rules of the GDPR for obliged entities . If the AML-CFT legislation is not designed in a balanced and proportionate manner, that respects every individuals' fundamental rights to data protection, legal uncertainties for obliged entities will continue to exist and the AML-CFT framework would be vulnerable. Data Protection Authorities will be forced to use their powers in order to bring the activities of the obliged entities in accordance with the GDPR through corrective measures. European citizens will also likely exercise their right to an effective remedy before a tribunal, enshrined in the Article 47 of the Charter of Fundamental Rights of the European Union.

Thus, the EDPB deems crucial to correctly articulate the interplay between the two legal frameworks, since such articulation is necessary to ensure the compatibility between personal data protection and the prevention of money laundering and terrorist financing. When properly addressed, the data protection principles could, moreover, lead to more efficiency of the AML-CFT framework, excluding inaccurate personal data from processing operations.

Yours sincerely,



Andrea Jelinek

CC: Ms Raluca PRUNA, Head of Unit, Unit D.2, DG FISMA

Mr Olivier MICOL, Head of Unit, Unit C.3, DG JUST

Letters



European Union Agency for Cybersecurity
Athens, Greece

Brussels, 09 March 2021
Ref: OUT2021-0047

ENISA published a draft version of the candidate European Cybersecurity Certification Scheme for Cloud Services (EUCS) on 22 December 2020. Following the publication, ENISA launched a public consultation on the draft scheme. The EDPB takes this opportunity to provide feedback on the EUCS candidate scheme, more specifically in relation to the potential synergies between the EUCS scheme with a view to supporting Cloud Service Customers (CSC) and Cloud Service Providers (CSP) to comply with the principles and rules established in the Regulation (EU) 2016/679 (GDPR)¹ with regard to the protection of personal data.

On the one hand, in accordance with Regulation (EU) 2019/881 (Cybersecurity Act)², cybersecurity aims at the *protection of “network and information systems, the users of such systems, and other persons affected by cyber threats”*, thereby also contributing to security of the processing of their personal data.

On the other hand, data protection rules laid down in the GDPR have as main objective the protection of natural persons with regard to the processing of their personal data. A key principle of the GDPR enshrined in article 5 (1) (f), imposes the respect of the ‘confidentiality and integrity’ of personal data undergoing processing. This key principle needs to be considered alongside article 32 of the GDPR that provides more specifically to the security of personal data processing.

The EDPB considers it important to identify and define synergies between the different tools that support data protection compliance and those that support information security. In this context, it is also important to ensure that the controls and requirements in the cybersecurity certification scheme do not conflict with the rules and principles of the GDPR. By doing so, adherence to these tools by the concerned stakeholders would also be facilitated.

In particular, the EDPB agrees with the approach adopted by the EUCS candidate scheme according to which the latter *“does not aim at verifying the compliance of a cloud service to any regulation beyond*

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

² Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

the EUCSA, and in particular it does not aim at verifying compliance with GDPR”. Moreover, Article 54 of the EU Cybersecurity Act states that the ‘*requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements*’. Furthermore, the EDPB also acknowledges the candidate scheme could contribute to facilitate compliance with the GDPR, i.e. in securing personal data processed by the cloud service provider, in line with the ‘confidentiality and integrity’ principle as per Article 5 (1) (f) GDPR.

The EDPB also welcomes the EUCS certification scheme initiative as tool to harmonize the security of cloud computing services at European level. The EUCS scheme will furthermore improve transparency on guarantees for security measures provided by a cloud service for public institutions, private companies and indirectly customers.

1. Personal data processing under the GDPR and security requirements

The EUCS scheme provides for a definition of “*cloud service customer data*”, “*cloud service derived data*” and “*cloud service provider data*” as classes of data objects categorized into non-critical, business critical and mission critical information.

In this regard, the EDPB recalls that Article 4 (1) GDPR provides for the definition of “*personal data*”³. Article 9 GDPR moreover defines the concept of “*special categories of personal data*”⁴. The latter is comprised of personal data, which are by their nature, particularly sensitive in relation to the fundamental rights and freedoms of natural persons and merit higher protection and security.

In light of the above, the EDPB notes that the EUCS scheme introduces classes of data objects that may include personal data, without referring to the concepts of personal data and special categories of personal data defined in the GDPR. Moreover, the EUCS scheme assurance levels are intended to minimize known basic risks of incidents and cyber-attacks up to risks of state-of-the-art cyberattacks carried out by actors with significant skills and resources, while data controllers are also required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk for the rights and freedoms of natural persons and taking into account the scope, context and purpose of the processing in order to comply with Article 32 GDPR (Security of processing).

Therefore, and since the risk inherent in processing of personal data is of varying likelihood and severity for the rights and freedoms of natural persons depends amongst others on the category of personal data processed, the inclusion of personal data and special categories of personal data into the EUCS scheme is even more critical.

³ According to Article 4 (1) GDPR, ““*personal data*’ means any information relating to an identified or identifiable natural person (‘*data subject*’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

⁴ Article 9 (1) GDPR defines special category data as “*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, a person’s sex life and data concerning a person’s sexual orientation*”.

Recommendation 1:

In order to provide an added value to the EUCS scheme and to ensure that -insofar as personal data are concerned- no inconsistencies with the definitions and concepts of the GDPR occur the EDPB suggests to introduce personal data and special categories of personal data as categories of data into the EUCS scheme, taking into account that derived data (not directly provided by data subjects) may be personal data. These two categories of data should also be taken into account to guide CSPs and CSCs when applying for an appropriate assurance level.

To further support the compliance with GDPR obligations by CSCs, and depending on the cloud capability type, the CSP may already be aware of the processing of personal data taking place in its cloud service. For example, an application cloud service, may process personal data as part of the service offered to the CSC (e.g. online HR software). For this type of service, the CSP should offer a level of security already adapted to the risks of this particular personal data processing and therefore have a certification with a level of assurance adapted to its context. Indeed, the GDPR requires processors to assist controllers⁵ in ensuring compliance with the obligations pursuant to Articles 32 taking into account the nature of processing and the information available to the processor.

Recommendation 2:

The EDPB suggests that the EUCS scheme encourages CSPs to choose for their certification a level of assurance that already takes into account, where applicable, the type of personal data likely or intended to be processed and the risks to the rights and freedoms of natural persons resulting from the processing carried out.

2. The differences between data protection rights (the right to data portability) and principles (confidentiality, integrity, transparency) and the security objectives (confidentiality, integrity, transparency, portability) in the EUCS candidate scheme

The EDPB also wants to stress the importance of the principles relating to processing of personal data set forth by Article 5 GDPR. Adequate security of personal data, mentioned in article 5 (1) (f) GDPR as the principle of ‘integrity and confidentiality’, is only one of them. Other principles must be considered when processing personal data, such as ‘lawfulness, fairness and transparency’, ‘purpose limitation’, ‘data minimization’, ‘accuracy’, ‘storage limitation’ and ‘accountability’.

For instance, in relation to the principle of transparency, the EDPB welcomes the inclusion of the “Complementary Customer Controls”⁶, according to which a CSP must provide information about the location of the processing and storage of data as well as the applicable law. Such information might help the CSC who wants to process personal data in the context of cloud computing services provided

⁵ Allocation of responsibilities for personal data processing in the context of cloud services has to be assessed on a case by case basis. The current EDPB guidelines on controller and processor in the GDPR can be found here:

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

⁶ Control DOC-03 LOCATIONS OF DATA PROCESSING AND STORAGE (pg. 151 of EUCS)

by the CSP to comply with security requirements and comply with the requirements of GDPR, especially with regard to the transfers of personal data to third countries⁷.

Recommendation 3:

The EDPB recommends including the requirements about the location of data processing in all assurance levels. Not including these requirements in the basic assurance level, as it is currently the case, would exclude this assurance level of the EUCS scheme to facilitate the compliance with GDPR for any personal data processing.

The principles mentioned above should guide all processing activities concerning personal data and are of particular relevance to allow data subjects to have control over the personal data relating to them, especially through the exercise of their rights as data subjects under the GDPR. For instance, the right to portability further strengthens the control of the data subjects over the personal data relating to them, by allowing them to receive personal data concerning them in a structured, commonly used, machine-readable and interoperable format, and to transmit those data to another controller. The high level of portability that can be achieved by the cloud service providers certified under EUCS candidate scheme meets different requirements than the right of portability in the GDPR.

Recommendation 4:

Therefore, the EDPB suggests clearly indicating in the scheme that the portability control in the EUCS scheme should not be confused with the right of portability in the GDPR.

The mandate received by ENISA to develop the EUCS candidate scheme is based on Article 54 of the EU Cybersecurity Act. This article states that the '*requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements*'. These legal requirements include the compliance with the data protection *acquis* when the cloud service provided by the CSP involves the processing of personal data.

Recommendation 5:

In this regard, the EDPB recommends the involvement of the CSP's Data Protection Officer (DPO) in the early stages of the designing of the service to assist the CSP to monitor internal compliance with the GDPR. By doing so, the security by design of the cloud service will be reinforced by contributing to the obligation of 'data protection by design'.

⁷ See, for example, Articles 13(1)(f), 14(1)(f) and 15(2) GDPR and more generally Chapter V of the GDPR.

The EDPB namely considers that the advice provided by the DPO to the CSP is an element that can positively contribute to the adoption of appropriate technical and organisational measures to safeguard the rights and freedoms of natural persons in the context of the EUCS candidate scheme and to ensure the consistency with the applicable legal requirements established by the EU Cybersecurity Act.

3. Extension of the audit rights for data controllers / processors

The EDPB welcomes that “*the CSP shall grant its CSCs contractually guaranteed information and define their audit rights*”.

Recommendation 6:

The EDPB recommends envisaging this possibility not only for the “High level” of assurance, but also for the “Basic” and for the “Substantial” levels of assurance. Not including this requirement in the “Basic” and “Substantial” assurance levels would exclude these assurance levels of the EUCS scheme from facilitating compliance with GDPR Article 28 (3) (h).

Therefore, it is also important to ensure that this possibility is clearly mentioned in the contract governing the provision of the cloud services between the CSP and the CSC, especially if it involves the processing of personal data. Not including this requirement in the “Basic” and “Substantial” assurance levels would exclude these level of certification to be used to facilitate compliance with Article 28 (3) (h) GDPR.

4. The EUCS scheme incident management requirements as support to the GDPR data breach requirements

Article 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 EUCS scheme requires in requirement IM-01.4 that “*The CSP shall inform the customers affected by security incidents in a timely and appropriate manner*”. Article 33(2) GDPR however requires that “*the processor shall notify the controller without undue delay after becoming aware of a personal data breach*”.

Recommendation 7:

The EDPB suggests adapting the wording of the EUCS requirements to reflect the GDPR requirements for personal data breaches and to make these requirements mandatory for all assurance levels of the

scheme. Not including these requirements in the “Basic” and “Substantial” assurance levels would preclude the use of these assurance levels of the EUCS scheme to facilitate compliance with GDPR Article 33 (Notification of a personal data breach to the supervisory authority).

5. The EUCS scheme as facilitator for GDPR Codes of conduct / certifications

By relying on a cybersecurity certification scheme harmonized at the European level, the private and public organizations that elaborate European or national codes of conduct or certification schemes, in accordance with Articles 40 and 42 GDPR, may support the applicants in demonstrating their compliance with such GDPR accountability tools. In particular, for applicants that rely on those GDPR accountability tools for the purpose of demonstrating compliance with the GDPR of their processing operations, the EUCS certificate or the related audit report may facilitate their assessment when identical or similar criteria are used in both tools.

Additionally, the EUCS scheme permits under certain conditions its assessment to a simplified methodology based on a self-assessment performed by the CSP. In this methodology, a conformity assessment body (CAB) can then audit the results of the self-assessment. As a consequence, if CSPs apply for a GDPR accountability tool that makes reference to some criteria of the EUCS scheme, the compliance to these criteria would need to be reassessed by a certification body or a monitoring body accredited, respectively, under Article 41 or 43 GDPR.

Recommendation 8:

Therefore, the EDPB suggests that all levels of the EUCS can benefit from equivalent proofs of compliance by allowing a fully independent third-party assessment. Not including this requirement would exclude the EUCS certificates or audit report based on the self-assessment methodology to facilitate compliance with GDPR accountability tools.

Conclusion

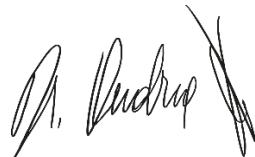
The EUCS certification may help supporting data protection security requirements and facilitate the adoption of this tool by stakeholders by:

- introducing a personal data category in the EUCS scheme;
- taking into account the notion of risks of personal data processing to the rights and freedoms of natural persons;
- reinforcing the EUCS security requirements needed to comply with the data protection rules on the security of processing;
- including in all assurance levels the GDPR security requirements mentioned in this letter. Excluding these requirements from some assurance levels of the EUCS scheme would result for the concerned assurance levels to not be usable to support compliance with GDPR requirements.

The above suggestion has only to be considered as a preliminary guidance. Assessments of the risks for personal data processing have to be done on a case-by-case basis under the responsibility of the data controller. Indeed, the GDPR accountability principle requires data controllers to take responsibility for what they do with personal data and how they comply with all the GDPR principles.

The EDPB remains open to any further discussion elaborating on how the EUCS certification scheme could contribute to facilitate compliance with the GDPR.

Yours sincerely,



Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Brussels, 12 September 2022

Ref.: OUT2022 -0068

Dear President Metsola,
Your Excellency Hrdá,

We, the Members of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), are writing to you regarding the 2023 budget, to call upon your support. We are deeply concerned that this budget, if not substantially increased, would be significantly too low to allow the EDPB and the EDPS to fulfil their tasks appropriately, as required by the General Data Protection Regulation (GDPR) and Regulation 2018/1725 (EUDPR).

The EDPB budget forms part of the broader budget of the EDPS*. The budget devoted to the EDPB for 2022 represents 6 812 000 euros and covers all aspects related to the functioning of the Board. This includes and is not limited to expenditure related to EDPB meetings at plenary and subgroup level, translation and interpretation costs, IT services, and remuneration of the EDPB Secretariat staff.

The EDPB Secretariat supports the Members of the Board by providing analytical, administrative and logistical support. In particular, it is responsible for the settlement of disputes between national data protection authorities (DPAs) within the One-Stop-Shop mechanism on draft decisions concerning private sector practices that may include fines amounting to several hundreds of millions of euros.

During the 2023 budget preparation, the EDPS made two consecutive budget proposals covering also the activities of the EDPB, which were both rejected by the European Commission. The second (reduced) proposal included a request for **8 additional staff members** (4 officials and 4 contractual agents) for the EDPB Secretariat in addition to its current 40 staff members, and **8 additional staff members for EDPS itself** (5 officials and 3 contractual agents). As for the EDPB only, the total requested budget for 2023 within this proposal was 7 766 000 euros. Although this would represent an increase of 14% compared to 2022, the budget remained 17% below the ceilings of the EDPS contribution to the Multi-Annual Financial Framework, which was adopted in 2020.

The EDPB is essential for the implementation of the GDPR, one of the landmark EU legislations of the last decades, which regulates a very high number of organisations processing personal data, including large companies such as big tech, SMEs, and the public sector. There are high expectations from society at large regarding the GDPR, especially with regard to its enforcement vis-a-vis big tech. However, the EDPB Secretariat is currently understaffed and at risk of no longer being able to fulfil its legal duties at the service of the EDPB and of the GDPR.

Should this happen, **the enforcement of individuals' data protection rights would be weakened and the credibility of the GDPR undermined.**

We call for your support in respect of the budget proposal, which aims at strengthening 3 essential pillars for the success of GDPR:

- the credibility of enforcement. As DPAs are developing their enforcement activities, this generates more disputes requiring the EDPB's intervention, a unique responsibility in the EU digital regulatory governance landscape. If the EDPB cannot settle a dispute within 2 months, the unilateral decision of the Lead Supervisory Authority will prevail, not taking into account the objections made by other Concerned Supervisory Authorities;
- the robustness of enforcement, as higher fines will inevitably lead to more litigation. The EDPB decisions must therefore meet very high quality standards and be able to withstand the legal firing power of technology companies, both of which require sufficient EDPB staff;
- the predictability of the legal framework, as the EDPB must continue to issue guidance to ensure and promote the harmonised application of the GDPR.

Moreover, the EDPB and the EDPS continue to receive new tasks from the legislator. The EDPB will be entrusted with the coordination of the supervision of the EU's large scale systems and agencies, while the EDPS is responsible for the actual supervision of the central components of the EU's large scale systems and of the EU agencies. The number of these systems and agencies will increase from 4 to date, to 12 by 2023, including Europol's information system, the Schengen system, the Visa information system, Eurodac and Etias. Moreover, the EDPS supervisory role and responsibilities on all European Institutions, bodies and agencies has increased considerably, also as a result of the expanded mandate of EUIs active in the Area of Freedom Security and Justice field (e.g. Europol) and the European Public Prosecution Office operations.

Finally, the EDPB and EDPS are increasingly consulted by the European Commission on legislative proposals, a role we consider crucial to ensure that data protection rights are upheld as the EU shapes its digital governance landscape. In 2021, the total volume of legislative consultations requests received by the EDPS essentially tripled in comparison to 2020, a trend which is expected to remain and grow in the future.

In light of the above, we strongly urge your support for our budget requests which include 8 additional staff members (4 officials and 4 contractual agents) for the EDPB Secretariat and 8 additional staff members (5 official and 3 contractual agents) for the EDPS Secretariat.

Fundamental rights are not to be taken for granted and require the appropriate human and financial resources to ensure their protection. We, as data protection authorities, are committed to working for the interests of individuals, and we hope you will share this commitment too.

Yours sincerely,

Dr Andrea Jelinek

Dr Wojciech Wiewiórowski

* References to the EDPS budget in this letter should be understood as also covering the EDPB Secretariat.

Cc:

Mr Didier REYNDERS, Commissioner for Justice
Mr Johannes HAHN, Commissioner for Budget and Administration
Mr Johan VAN OVERTVELDT, Chair, Committee on Budgets (BUDG)
Ms Monika HOHLMEIER, Chair, Committee on Budgetary Control (CONT)
Mr Juan Fernando LOPEZ AGUILAR, Chair, Committee on Civil Liberties, Justice and Home Affairs (LIBE)
Mr. Niclas HERBST, Member of the European Parliament, rapporteur on Parliament's estimates of revenue and expenditure for the financial year 2023
Mr Serge DE BOLLEY, Director for Justice, Secretariat General of the Council
Mr Olivier MICOL, Head of data protection unit, Directorate General for Justice and Consumers, EU Commission

Memorandum of Understanding between the European Data Protection Board and the European Data Protection Supervisor

I. Purpose of this document

1. Independent data protection authorities in the European Union are cooperating in a spirit of trust, good faith and collegiality.
2. The General Data Protection Regulation (EU Regulation 679/2016, hereinafter ‘GDPR’)¹ reinforces the terms for this cooperation by the creation of a new European body, the European Data Protection Board (hereinafter ‘EDPB’), to be composed of all national supervisory authorities and the European Data Protection Supervisor (hereinafter ‘EDPS’).
3. The EDPB is an EU body with legal personality that acts independently (Article 69.1 of the GDPR) when performing the tasks described in Articles 70 and 71 of the GDPR. Article 51 of the Data Protection Directive² (hereinafter ‘DPD’) and other relevant applicable EU law.
4. The EDPS is an independent EU supervisory authority with legal personality that acts in complete independence in the performance of its duties (Articles 41.1 and 44.1 of Regulation 45/2001³). The EDPS is recognised as an EU institution in the Financial Regulation applicable to the general budget of the Union and its rules of application⁴ and therefore benefits from budgetary autonomy. The tasks of the EDPS are defined in Regulation 45/2001 (Articles 41.2 and 46).

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA.

³ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

⁴ Regulation (EU, EURATOM) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002,
<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0966&from=en>.

5. Article 75 of the GDPR stipulates that the Secretariat of the EDPB will be provided by the EDPS, which involves taking on responsibilities for organisational matters in order to support the providing of the Secretariat, in line with Article 44 of the Regulation 45/2001⁵ and Article 69.1 of the GDPR, including on matters where the EDPB, although being an EU body with legal personality, cannot legally adopt the decisions such as budget, human resources and financial administration.
6. The GDPR states that the Secretariat shall perform its tasks exclusively under the instructions of the Chair. The EDPS staff involved in carrying out the tasks conferred to the Board shall be subject to separate reporting lines from staff involved in carrying out tasks conferred to the EDPS (Article 75.3).
7. Given the positive spirit of cooperation among the community of supervisory authorities in the EU, the EDPB and the EDPS have agreed that a Memorandum of Understanding (hereinafter 'MoU') serve as a valuable guide and additional point of reference as to the common commitment of the EDPB and the EDPS concerned towards sound administrative management and synergies and the effectiveness of the EDPB.
8. This MoU also applies to the staff of the EDPS carrying out the tasks supporting the EDPB for implementing the DPD Article 51.1 and other relevant applicable EU law.

II. Definitions

In this document:

1. "Party" means the EDPS or the EDPB, all together referred as "the Parties";
2. "Staff" means officials, contract agents, seconded national experts, temporary agents and trainees hired according to Staff Regulation 31 (EEC), 11 (EAEC), which lays down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community⁶;
3. "Secretariat" means the Secretariat of the EDPB according to Article 75 of the GDPR;
4. "Secretariat staff" consists of members of staff of the EDPS, including the Head of Secretariat provided by the EDPS, carrying out analytical, administrative and logistical tasks to support the EDPB exclusively under the instructions of the Chair of the EDPB and subject to separate reporting lines as provided in Article 75 of the GDPR;
5. "EDPS staff" means members of staff who carry out tasks conferred on the EDPS and work exclusively under the instructions of the Supervisor;
6. "Supervisor" means the Supervisor of the EDPS;
7. "Director" means the Director of the EDPS both in his or her capacity as Appointing Authority and Authorising Officer by Delegation, pursuant to Articles 9 and 10 of the Rules of Procedure - Decision of the EDPS;⁷

⁵ In particular, paragraph 1 and 2 ("1. *The European Data Protection Supervisor shall act in complete independence in the performance of his or her duties.* 2. *The European Data Protection Supervisor shall, in the performance of his or her duties, neither seek nor take instructions from anybody*").

⁶ Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01962R0031-20140501>

⁷ Rules of Procedure - Decision of the EDPS of 17 December 2012 on the adoption of Rules of Procedure, [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0504\(03\)&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0504(03)&from=EN)

8. "Head of Secretariat": means a staff member of the Secretariat responsible for coordinating the work of the Secretariat;
9. "Chair" means the EDPB elected chair.

III. Principles

The terms of this MoU are underpinned by the following principles:

- (i) independence and impartiality of action of the EDPB and the EDPS in performing their tasks and powers;
- (ii) good governance, integrity and good administrative behaviour in acting in the public interest;
- (iii) collegiality;
- (iv) cooperation and endeavouring to operate by consensus;
- (v) confidentiality for restricted information
- (vi) efficiency and modernisation to ensure the highest level of synergies;
- (vii) proactivity in anticipating and supporting modern, future-oriented solutions to the new digital challenges to data protection.

IV. The tasks of the Secretariat

1. Under Article 75.5 of GDPR, the Secretariat is required to provide analytical, administrative and logistical support to the EDPB.
2. Article 75.6 of the GDPR provides for a list of tasks to be carried out by the Secretariat. These tasks will allow the Secretariat to effectively carry out the support function foreseen in Article 75.5. Those tasks also include:
 - (i) the organisation of EDPB meetings (sending invitations, booking rooms, catering, gathering evidence and preparing of the reimbursement of travel costs and drafting the agenda and the minutes);
 - (ii) providing further development, use, maintenance and support for the EDPB IT communication tool and One Stop Shop communication tool (covering the EDPB IT system);
 - (iii) the handling of public access to documents requests;
 - (iv) record management;
 - (v) security of information (LISO);
 - (vi) ensuring information and communication tasks, such as maintaining press relations and the drafting/publication press releases, producing web or social media content, briefings, speeches, blog posts, audio-visual material and presentations (communication);
 - (vii) ensuring public relations with other institutions, including representation of the Board before the courts, in accordance with the Rules of Procedures;
 - (viii) the Data Protection Officer's (DPO) activities;

- (ix) Providing the translation of the relevant documents, in accordance with the Rules of Procedure of the EDPB.
3. Certain activities mentioned in paragraph 2, such as translations and interpretation, will be provided by other EU institutions or bodies under SLAs. Where it is identified that existing or new SLAs concluded by the EDPS with other EU institutions or bodies are relevant to the EDPB, the EDPS will involve the EDPB in any (re)negotiation.
 4. The EDPB and EDPS DPOs will meet regularly in order to ensure that their decisions remain consistent.

V. Internal organisation of the Secretariat – Cooperation and Confidentiality

1. The Chair of the Board is tasked, inter alia, with ensuring the timely performance of the tasks of the Board and shall be assisted by the Secretariat to perform this task.
2. The Secretariat staff are separated from EDPS staff. This means that they are subject to separate reporting lines and that the Secretariat will consist of Secretariat staff only.
3. Should any matter of relevance for the EDPB concern both Parties, the Secretariat staff and the EDPS staff, the Supervisor and the Chair shall work together to reach consensus and to find solutions which are in the best interest of both parties and their respective staff.
4. The Head of Secretariat and the EDPS Head of Human Resource, Budget and Administration Unit will meet regularly to ensure full synergy, coherence and consistency in the administrative management of the EDPB and the Secretariat, and to safeguard the administrative accountability of the EDPS. These meetings will enable the Parties to better share administrative information and improve best practices on budget implementation, procurement, expenditures, logistics and good administration. The Chair may make, in principle via the Head of Secretariat, any request to the EDPS Head of Human Resource, Budget and Administration Unit concerning the administrative management of the EDPB and the Secretariat.
5. The Secretariat staff must also act according to the requirements and best practices established in the EDPS Code of Conduct⁸.
6. The Secretariat staff will be located in dedicated offices separated from the offices of the EDPS staff to which access will be restricted. They will have specific e-mail addresses (XX@edpb.europa.eu) and all official documents produced by the Secretariat will be formally identified as EDPB documents.
7. Without prejudice to the professional secrecy⁹, the Parties agree to exchange on a regular basis relevant information to make this MoU effective.

⁸Code of Conduct:

<http://www.edpsnet.ep.parl.union.eu/edpsnet/webdav/site/edpsnet2/shared/HRAB/Documents/code%20of%20conduct.final.pdf>.

⁹ For EDPS staff, including the Secretariat staff, Art 17 of the Staff Regulation, Article 45 of Regulation 45/2001 on the basis of Article 339 of the Treaty on the Functioning of the European Union will be applicable. For national supervisory authorities staff, Article 54.2 of the GDPR and 44.2 of the DPD will apply.

8. To maintain mutual trust through the sharing of information flow in both directions, the Parties:
 - (i) will ensure that any sensitive non classified information and classified information will only be exchanged and used exclusively for lawful purposes and only where relevant for the respective duties of the Parties, in compliance with relevant EDPS and EDPB Decisions on Security and according to EU standards;
 - (ii) will restrict access where appropriate to ensure the separation of functions and the sensitivity of information;
 - (iii) will respect confidentiality and security rules, preventing any unauthorised access to restricted information.
9. Similarly, IT systems and tools used by the Secretariat should be designed in a way which mitigates the risk of security breaches. The same rules shall apply to external staff performing tasks for the Secretariat through ad hoc contractual clauses imposing the same confidentiality rules and the Information Security Policy of the EDPB will provide for the necessary access restrictions which are implemented in relevant IT systems.
10. In the case of a breach of the EDPB or EDPS Security Rules, with regards to the EDPB information or to the implementation of the MoU, the Chair and the Director will be notified after the intervention of the respective Local Information Security Officer (LISO) and the EDPS Local Security Officer (LSO), so that appropriate action may be taken.

VI. EDPS responsibilities to provide the Secretariat

1. To provide the Secretariat, the EDPS will:
 - (i) provide **separate staff** to carry out tasks conferred to the Secretariat. The EDPS will take all reasonable measures to provide suitable staff in accordance with the needs identified by the EDPB. The EDPS will also provide Human Resources support, including selection, recruitment, payroll, appraisal, promotion, learning and development, mission organisation, respect for ethics and leave requests for the Secretariat staff;
 - (ii) provide a **working place** to staff carrying out tasks conferred on the Secretariat;
 - (iii) provide a **working infrastructure** to Secretariat including all reasonable and necessary communications and working equipment necessary for the EDPB Secretariat;
 - (iv) provide **financial resources and support** to the EDPB and the Secretariat. The EDPS will prepare, defend and implement the budget dedicated to the EDPB. The EDPS Annual Activity Report foreseen in Article 66.9 of the EU Financial Regulation will cover the budget dedicated to the EDPB and the EDPS will be responsible for the Internal Control Coordination function;
 - (v) ensure the **security** of the building via appropriate arrangements.
2. Where necessary, the EDPS may decide, after informing the EDPB, that one or several of the services mentioned in paragraph 1 such as payroll or the basic IT infrastructure made available to the Secretariat, will be supplied by other EU institutions or bodies under SLAs. The EDPS will consult the EDPB on any (re)negotiation and the EDPS will take utmost account of its opinion and give reasons why when taking a different position than the one expressed by the EDPB.
3. The EDPS will inform and consult the EDPB in advance where there is any matter of relevance for the EDPB and its functioning.
4. In addition, in all matters foreseen in paragraphs 5, 6 and 7, the EDPS, before taking a decision of relevance to the EDPB, will take utmost account of any opinion of the Board and endeavour to reach consensus. If consensus cannot be achieved, the EDPS will give reasons for not following the opinion of the EDPB.

5. On HR matters, a close cooperation with the Chair will take place in the definition of job profiles according to the EDPB needs and in the organization of the selection procedure of the Secretariat staff, in compliance with the EU staff regulations. Recruitment, appraisals and promotions will be carried out in accordance with the provisions of the Staff Regulations and the EDPS implementing decisions. Missions and trainings will be authorised by the Head of Secretariat and validated by the Authorising Officer by Delegation to ensure respect of the budget and of EU regulations.
6. For budget matters, a dedicated Title in the EDPS budget differentiates as much as possible resources and expenses of the EDPS from those of the EDPB. The EDPS will work in close cooperation with the Chair regarding the formulation and adoption of the EDPB budget on the basis of justified needs and after the consultation of the EDPB.
7. As regards the expenditure of the EDPB, the Head of Secretariat will act as operating agent deciding *de facto* on the commitments and expenditure of the EDPB. The expenditures will be executed and signed by the EDPS after verifying that the budget and EU Financial Regulations are respected. In case the EDPS refuses to execute an item of expenditure or decide differently than the views of the EDPB, for example to comply with a formal requirement under EU law, the EDPS will explain its decision to the Head of Secretariat.

VII. Additional functions performed by the EDPS to cooperate with the Secretariat

1. In order to enhance synergies, savings and economies of scale, the EDPS will ensure the technical tasks for EDPB information and administrative communication, such as:
 - (i) providing the technical development and assistance for the **EDPB website**;
 - (ii) producing audio-visual material;
 - (iii) providing technical support for events and study visits;
 - (iv) publishing, and sending documents promptly, such as news, press releases, speeches, blog posts, document, web content, upon request of the Head of Secretariat (because, for example, the person responsible for the publication of documents within the Secretariat is not available).
2. The EDPS Head of Information and Communication will be responsible for organising those tasks relating to EDPB activities as requested by the Head of Secretariat.
3. The EDPS Head of Information and Communication will cooperate with the Head of Secretariat when conducting appraisals and promotion exercises concerning his/her members of staff who also work on tasks relating to EDPB activities.

VIII. Implementation, revision and amendments

The Parties will meet regularly, at least once a year, in order to exchange views on the practical implementation of the working arrangements and may decide to amend this MoU.

IX. Entry into force and publication

This MoU will apply on the day following the date of its signature and its initial and amended version shall be published in the Official Journal of the European Union and on the websites of the Parties pursuant to Article 75(4) of the GDPR.

Drawn up at Brussels on 25 May 2018 in two original copies each in the English language and signed by the EDPB Chair and by the Supervisor.

For the European Data Protection Board

[signed]

Name:

25. 5. 2018

For the European Data Protection Supervisor

[signed]

Name:

A. von Bunkhorst

Opinion of the Board (Art. 64)



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 article 41 GDPR

Adopted on 23 March 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 NO 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	EXPERTISE	7
2.2.4	ESTABLISHED PROCEDURES AND STRUCTURES	7
2.2.5	REVIEW MECHANISMS	7
2.2.6	LEGAL STATUS	7
2.2.7	SUBCONTRACTING	7
3	CONCLUSIONS / RECOMMENDATIONS.....	8
4	FINAL REMARKS.....	8

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 2018,¹

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

¹ 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 Norwegian Supervisory Authority (hereinafter "NO 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 26 January 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 NO SA to take further action.
7. This opinion does not reflect upon items submitted by the NO 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 NO 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 is of the opinion that examples help in understanding draft requirements. Therefore, the Board encourages the NO SA to include in the draft accreditation requirements, some additional examples. In particular, the Board encourages NO SA to add:
 -]) example of ad hoc internal committee as an internal monitoring body (introduction);
 -]) examples of services to code members or to the code owner that can adversely affect its independence (section 1.1.4);
 -]) examples of ways of ensuring impartiality in relation to accountability during the application process (section 1.4.3).
10. In paragraph “duration of accreditation” in the introduction, the Board notes that the reference to the periodic review does not mention that the NO SA will review the compliance with the requirements

periodically. Thus, the Board encourages the NO SA to specify the possible duration of the accreditation (for example in years or for an indefinite period of time), 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.

11. The Board observes that the NO SA's draft accreditation requirements sometimes refer to an obligation ("shall") and sometimes to a possibility ("should"). For the sake of clarity, the Board recommends that the NO SA avoids the use of "should" in the text of the accreditation requirements.

2.2.2 INDEPENDENCE

12. As regards the monitoring body's independence in relation to legal and decision-making procedures, the Board underlines that it should exist not only towards the code owner, but also towards the members of the code. Thus, in section 1.1.5.h, the Board encourages making a clear reference that the independence may be demonstrated also by documents providing evidence of the business, financial, contractual, or other relations between the monitoring body and not only the code owner but also the members of the code.
13. In section 1.2.2, with respect to internal monitoring bodies, the Board encourages NO SA to add a requirement to prove that a specific separated budget is allocated to such bodies by the code owner.
14. 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. That is why, with respect to section 1.2.4 of the draft requirements, the Board encourages to NO 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.
15. 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 (subsection 1.2.3). 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 NO SA to provide examples of how the monitoring body can provide such evidence.
16. With respect to section 1.4.1 and demonstrating accountability by the monitoring body, the Board considers that the requirements should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate its accountability. In this regard, the Board notes the example provided as to how to accomplish accountability. However, the Board believes that the example could be developed in order to make a clear reference to setting out the roles and decision-making framework and reporting procedures, and setting up policies to increase awareness among the personnel about the governance structures and the procedures in place. Thus, the Board encourages the NO SA to develop the example in this sense.

2.2.3 EXPERTISE

17. With respect to section 3.3 the Board encourages the NO SA to add examples of documentation related to the expertise of the personnel in data protection, such as trainings and data protection certificates.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

18. The Board shares the view of the NO SA whereby the monitoring body must establish procedures to assess the eligibility of controllers and processors to comply with the code. At the same time, the monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of the members within a clear time frame, and check the eligibility of members prior to joining the code. Therefore, the Board recommends the NO SA to reflect this in the text.

2.2.5 REVIEW MECHANISMS

19. As regards section 7.3, the Board is of the opinion that the monitoring body should be able to contribute to reviews of the code as required by the code owner and shall therefore 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 and continues to adapt to any changes in the application and interpretation of the law and new technological developments. Therefore, the Board encourages the NO SA to reflect in the text that both, changes in the application and interpretation of the law and new technological developments, need to always be taken into consideration.

2.2.6 LEGAL STATUS

20. In section 8.2, the Board encourages the NO SA to specify that capability of being held legally responsible for monitoring activities should include that fines per Article 83(4)(c) GDPR can be imposed on the monitoring body and met.
21. In section 8.5, the Board encourages the NO SA to make a clear connection between the first and the second sentence of this section.
22. With respect to section 8.6, the Board agrees with the NO SA that a natural person must demonstrate adequate resources that allow it to act as a monitoring body. The Board encourages the NO 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.

2.2.7 SUBCONTRACTING

23. As regards section 9 the Board considers that the monitoring body, in addition to be the ultimate responsible for the decision-making, is also responsible for compliance when it uses subcontractors. The Board encourages the NO SA to add the reference to compliance. Moreover, the Board encourages

NO SA to include a clear requirement for subcontractors to comply with their data protection obligations.

24. In section 9.2, the Board recommends the NO SA to add a clear indication that 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 NO SA to add such remark. Finally, the Board encourages the NO SA to clarify the meaning of the sentence starting with “can be demonstrated”.

3 CONCLUSIONS / RECOMMENDATIONS

25. The draft accreditation requirements of the Norwegian Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
26. Regarding “general remarks” the Board recommends that the NO SA:
- avoid the use of “should” in the text of the accreditation requirements.
27. Regarding “established procedures and structures” the Board recommends that the NO SA:
- add a clear indication that the monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear time frame, and check eligibility of members prior to joining the code.
28. Regarding “subcontractors” the Board recommends that the NO SA:
- add a clear indication that the monitoring body shall ensure effective monitoring of the services provided by the contracting entities.

4 FINAL REMARKS

29. This opinion is addressed to the Norwegian supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
30. According to Article 64 (7) and (8) GDPR, the NO 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.
31. The NO 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 1/2022 on the draft decision of the Luxembourg
Supervisory Authority regarding the GDPR – CARPA
certification criteria**

Adopted on 1 February 2022

Table of contents

1	SUMMARY OF THE FACTS	4
2	ASSESSMENT.....	5
2.1	General remarks	5
2.2	Scope of the certification mechanism and Target of Evaluation (ToE).....	6
2.3	Procedure to determine a Target of Evaluation (ToE)	6
2.4	Certification criteria	7
2.5	Lawfulness of Processing	8
2.6	Principles of Article 5	10
2.7	General Obligations for Controllers and Processors	10
2.7.1.	Obligation applicable to controllers and processor	11
2.7.2.	Obligations applicable to the controllers	12
2.7.3.	Obligations applicable to processors	13
2.8	Rights of data subjects	13
2.9	Risks for the rights and freedoms of natural persons and technical and organisational measures guaranteeing protection	14
3	CONCLUSIONS / RECOMMENDATIONS	15
4	FINAL REMARKS	18

The European Data Protection Board

Having regard to Article 63, Article 64(1)(c) and Article 42 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 2018¹,

Having regard to Article 64(1)(c) of the GDPR and Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) Member States, supervisory authorities, the European Data Protection Board (hereinafter “the EDPB”) and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms (hereinafter “certification mechanisms”) and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises². In addition, the establishment of certifications can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services³.
- (2) The certification criteria form an integral part of any certification mechanism. Consequently, the GDPR requires the approval of national certification criteria of a certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b) of the GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) of the GDPR).
- (3) When a supervisory authority (hereinafter “SA”) intends to approve a certification pursuant to Article 42(5) of the GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR, through the consistency mechanism referred to in Articles 63, 64 and 65 of the GDPR. In this framework, according to Article 64(1)(c) of the GDPR, the EDPB is required to issue an Opinion on the SA’s draft decision approving the certification criteria.
- (4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis “Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation” (hereinafter the “Guidelines”) and their Addendum providing “Guidance on certification criteria assessment” (hereinafter the “Addendum”), for which the public consultation period expired on 26 May 2021.

¹ References to “Member States” made throughout this Opinion should be understood as references to “EEA Member States”.

² Article 42(1) of the GDPR.

³ Recital 100 of the GDPR.

- (5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.
- (6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR; therefore, the certification criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.
- (7) At the same time, the certification criteria should take into account and, where appropriate, be inter-operable with other standards, such as ISO standards, and certification practices.
- (8) As a result, certifications should add value to an organisation by helping to implement standardized and specified organisational and technical measures that demonstrably facilitate and enhance processing operation compliance, taking account of sector-specific requirements.
- (9) The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency.
- (10) The EDPB recalls that certifications are voluntary accountability tools, and that the adherence to a certification mechanism does not reduce the responsibility of controllers or processors for compliance with the GDPR or prevent SAs from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.
- (11) The Opinion of the EDPB shall be adopted, pursuant to Article 64(1)(c) of 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 SA 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.
- (12) The EDPB Opinion focusses on the certification criteria. In case the EDPB requires high level information on the evaluation methods in order to be able to thoroughly assess the auditability of the draft certification criteria in the context of its Opinion thereof, the latter does not encompass any kind of approval of such evaluation methods.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with Article 42(5) of the GDPR and the Guidelines, the “GDPR-CARPA certification criteria” (hereinafter the “draft certification criteria” or “certification criteria”) was drafted by the Luxemburg Supervisory Authority (hereinafter the “LU SA”).
2. The LU SA has submitted its draft decision approving the GDPR-CARPA certification criteria, and requested an Opinion of the EDPB pursuant to Article 64(1)(c) GDPR on 1 October 2021. The decision on the completeness of the file was taken on 28 October 2021.

The present certification is not a certification according to article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or

international organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V of the GDPR are respected.

2 ASSESSMENT

3. The Board has conducted its assessment in line with the structure foreseen in Annex 2 to the Guidelines (hereinafter “Annex”) and its Addendum. Where this Opinion remains silent on a specific section of the LU SA’s draft certification criteria, it should be read as the Board not having any comments and not asking the LU SA to take further action.

2.1 General remarks

4. The Board notes that the terms used throughout the document can sometimes be confusing. An example regarding the consistency of the terminology can be found under section I-13, where there is a reference to “persons concerned”, which should be replaced with “data subjects”. Therefore, the Board encourages the LU SA to ensure the consistency of the term used throughout the draft certification criteria.
5. The Board encourages to clarify the meaning of some of the terms used in the certification criteria, such as the entity’s “authorized” management that is required to supervise the implementation of the mechanism supported by its DPO for international data transfers so as to ensure their compliance with the GDPR (see criteria II-a-18 and III-13, but also I-1) and the “formal assessment” required to be performed by the entity as it is mentioned several times throughout the draft criteria (e.g. section II-a-10).
6. The draft criteria state in several sections that “the entity has taken into account the formal opinion of its DPO” (e.g. sections II-a-18 and III-13). The Board encourages the LU SA to clarify, in a note in the draft criteria, that the DPO, even if he/she has a significant role for the compliance monitoring of the entity’s processing activities according to Article 39 of the GDPR, the latter should not be the one responsible to assess the implementation of the measures designed to ensure such compliance.
7. The Board notes that the certification criteria submitted by the LU SA do not contain any information on the planned evaluation methods. According to the LU SA, these can be derived (in part) from the International Standard on Assurance Engagements (ISAE 3000 standard), which is part of the certification process as it is used in connection with the accreditation. Based on the information provided by the SA, this standard has been developed by the International Auditing and Assurance Standards Board (IAASB) and deals with assurance engagements other than audits or reviews of historical financial information. The EDPB encourages the LU SA to clarify that the ISAE 3000 standard is not of relevance for the certification criteria as it is not part of it, but it is relevant for the certification process. In this regard the EDPB recalls what already recommended in the context of its Opinion on the accreditation requirements for LU SA’s certification bodies.⁴

⁴ See EDPB Opinion 5/2020 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 Article 43(3) (GDPR), adopted on 29 January, para. 8.

2.2 Scope of the certification mechanism and Target of Evaluation (ToE)

8. The GDPR-CARPA certification scheme is a general scheme in that does not focus on a specific sector or type of processing. According to the information provided by LU SA, the main object of the certification scope are the data protection responsibilities of the controller / processor (accountability principle). For this reason, the GDPR-CARPA includes requirements focusing on the data protection governance in the organization surrounding the processing activities included the TOE in addition to specific criteria concerning directly those processing activities. However, the LU SA established some scope limitations / exclusions to clarify which (type of) processing activities can / cannot be certified under GDPR-CARPA certification scheme. In particular, GDPR-CARPA is not suitable for:

- certifying personal data processing specifically targeting minors under 16 years old;
- certifying processing activities in the context of a joint controllership;
- certifying processing activities in the context of article 10 GDPR;
- entities that have not officially designated a DPO (article 37 GDPR).

In this regard, the Board notes that the GDPR CARPA scheme does not mention the exclusion of processing activities falling under Articles 85 to 89 GDPR. However, the Board understands that relevant aspects of GDPR compliance with regard to the processing operations falling under those Articles are meant to be covered by the certification criteria. For example, section II-a-9 of the draft certification criteria concerns the processing of special categories of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, but it does not mention the suitable and specific measures to safeguard the fundamental rights and interests of data subjects required under Article 89(1) of the GDPR. Therefore, the Board recommends the LU SA to include specific criteria covering processing activities under Articles 85 to 89 of the GDPR.

Furthermore, the Board recommends the LU SA to include that an analysis of the relevant laws shall be performed by the entity which demonstrates that specific and suitable measures have been put in place in order to respect the fundamental rights and interests of data subjects pursuant to Article 89 of the GDPR.

2.3 Procedure to determine a Target of Evaluation (ToE)

9. According to the information provided by the LU SA, the TOE for the certification has to be setup following the “Planning and Performing the Engagement” requirements of the International Standard on Assurance Engagements (ISAE standard), which is part of the certification process. However, as stated in the EDPB Guidelines 1/2018, how the ToE has to be defined should be sufficiently described in the certification criteria themselves (see Annex 2 to the EDPB Guidelines 1/2018, section 2.f). This seems not to be the case for the GDPR-CARPA certification scheme which in this regard relies on the ISAE standard, while provides guidance to define the TOE in the certification program. In this context, the Board recommends the LU SA to include in the beginning of the draft certification criteria, in a devoted section, sufficient information with regard to the criteria on how the ToE is defined.

2.4 Certification criteria

10. The Board notes that in a large number of the criteria it is not clear what needs to be audited and by whom. On the contrary, the Board, underlines that this should be made clear from the criteria themselves. In particular, the tool of “self-assessment” by the applicant is used in many criteria. In this regard, the Board notes that the LU SA does not always define in the criteria the elements upon which the self-assessment should be carried out by the applicant so as to make clear what is expected to be demonstrated by the applicant and audited by the certification body. For example, sections II-a-1 and II-a-4 about identification of a valid legal basis and data processing based on contract respectively do not specify the factors that should be taken into account by the applicant when carrying out the assessment on the identification of the legal basis, such as the necessity of the processing in relation to the purposes pursued and the appropriateness of the legal basis considering the processing activities, depending on the nature, context, scope and purposes of the processing. The same applies to the other criteria concerning the rest of the legal grounds (i.e. II-a-3 and II-a-5-8).

In that respect, it should be avoided that the certification body takes over the assessment of the applicant without checking or at least critically questioning it with regard to the said factors to be specified in the criteria. This applies in particular to the criteria listed below:

- Section II-a-1 and II-a-3 to II-a-8 with regard to the above-mentioned factors regarding the assessment on the identification of the legal basis of the data processing.
- Section I-14 regarding data breaches in relation to the factors to be taken into account for the required assessment.
- Similarly, in section I-15 regarding the notification of data breaches towards the controller, with reference to the factors to be considered in the context of the assessment of those breaches.
- Section II-a-11 regarding the rights to restriction of the processing, with respect to the factors to be taken into account, to establish the impossibility or disproportionate character of the communication to the recipients to whom personal have been disclosed.
- Similarly, in section II-a-14 regarding the factors to be taken into account to determine if the provision of information to data subjects in accordance with Article 14 of the GDPR proves impossible or would involve a disproportionate effort.
- Section II-a-18 regarding third country transfers, see the specific recommendation in paragraph 22 of this Opinion.
- Section II-b-2 regarding purpose compatibility, see the specific recommendation in paragraph 23 of this Opinion.
- Section II-c-2 regarding alternative means, with respect to the factors be taken into account when assessing whether there is an impossibility to reach the purposes by implementing a less intrusive process (e.g. amount of data collected, retention period, aim of processing, technology available).

- Section II-d-3 regarding the right to rectification, in relation to the factors on which the assessment of impossibility or disproportionate character of the communication to the recipients to whom personal have been disclosed should be based.
- Section II-e-1 regarding the defined retention period omits to provide the factors that should be taken into account in case the retention period cannot be established in light of the applicable legal requirements (e.g. purpose(s) pursued).
- Section II-e-3 regarding the right to erasure, with reference to the factors to consider in the assessment of the impossibility or disproportionate character of the communication to the recipients to whom personal have been disclosed.
- Section II-f-2 regarding the risk analysis, see the specific recommendation in paragraph 52.
- Section II-f-9 regarding the assessment of sufficiency, see the specific encouragement in paragraph 35.
- Section III-7 regarding the risk treatment see the specific recommendation in paragraph 55.
- Section III-3 regarding the transfers to third countries, see the specific recommendation in paragraph 22.

Therefore, the Board recommends the LU SA to amend the above-mentioned criteria to provide the factors that shall be taken into account by the applicant when carrying out the relevant assessments so as to also clarify what will be checked by the certification body.

2.5 Lawfulness of Processing

11. The Board notes that under section II-a-1, the LU SA makes reference to a “valid legal basis”. However, the Board is of the opinion that the LU SA should take into account how the applicability of the legal basis is demonstrated and its appropriateness, where relevant, considering the processing activities, depending on the nature, context, scope and purposes of the processing. The Board recommends the LU SA to modify this criterion accordingly.⁵
12. Under section II-a-3 it is mentioned that “the entity has analysed the necessity of consent”. The Board recommends the LU SA to take into account that the entity demonstrates the appropriateness of consent as the legal ground for the processing in the individual case, instead of its necessity so to have this criterion in line with Recital 43 of the GDPR and the EDPB Guidelines on consent under the GDPR.⁶
13. Under section II-a-3, regarding “freely given” consent the Board encourages the LU SA to add a reference to Recital 32 for completeness.

⁵See Recital 43 of the GDPR as well as the EDPB Guidelines 05/2020 on consent under the GDPR available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

⁶ See for instance paragraphs 2, 3, 16, 17, 31 and 91 of the EDPB Guidelines 05/2020 on consent under the GDPR available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

14. The Board takes note of the requirement of informed and unambiguous consent in section II-a-3. However, the Board considers that more information is needed thereof. More precisely, the Board recommends that the LU SA adds in its draft certification criteria the minimum requirements which have to necessarily be met so that consent can be considered informed and unambiguous and that the criteria bring sufficient added value for the compliance with the GDPR of the certified entities.
15. Under section II-a-8, the draft certification criteria state: "The legislator provides by law for the legal basis for public authorities to process personal data". Consequently, this legal basis should not apply to the processing by public authorities in the performance of their tasks". In this regard, the EDPB encourages the LU SA to replace the word "should" with "shall".
16. The Board notes that in section II-a-9, regarding the processing of special categories of personal data, the reference to appropriate safeguards, when Article 9(2) of the GDPR provides so, is missing. For example, with respect to the processing, which is necessary for reasons of public interest (Article 9(2)(i) of the GDPR) in the area of public health, the suitable and specific measures provided for by Union or Member State law to safeguard the rights and freedoms of data subjects, in particular professional secrecy must be in place. The Board recommends the LU SA to take into account such safeguards, where necessary throughout this section and modify these criteria accordingly.
17. More in detail, with respect to section II-a-9 referring to Article 9(2)(b) of the GDPR, it is mentioned that "the entity has identified the applicable legal basis and formally assessed its applicability with regard to this processing activity". The EDPB recalls that the controller is authorised for such processing by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject. The EDPB considers that, without taking into account all the elements of compliance provided by this provision, such as the safeguards adhered to by the controller, the certification body's checks and controls would not be concrete enough, considering that the criterion where the assessment relied on is insufficiently detailed. Therefore, the Board recommends the LU SA to modify this criterion accordingly so to allow the certification body's assessment to be exhaustive.
18. Similarly, concerning the "legitimate activities by a foundation, association or any other non-for-profit body [...]" the Board recommends to take into account the appropriate safeguards required by Article 9(2)(d) of the GDPR.
19. Along the same lines, with respect to Article 9(2)(g) of the GDPR regarding the "substantial public interest" the mere reference in the criteria to the identified Union or Member States law(s) is not sufficient. The "specific measures to safeguard the fundamental rights and interests of the data subject" should also be taken into account and ensured to exist in this context. Therefore, the Board recommends to consider such elements in the draft certification criteria to provide sufficient added value for the certified entities in terms of compliance with the GDPR.
20. Similarly, under the same section, the Board notes that there is no reference to further conditions, including limitations regarding the processing of genetic data, biometric data or data concerning health. The Board recommends that the LU SA modifies this criterion accordingly so as to refer to the elements of compliance with the GDPR pursuant to Article 9(4), where relevant.

21. With regard to section II-a-18 concerning the transfer of personal data to third country, the Board recommends that the LU SA includes a reference to Articles 44-45 of the GDPR in the “Label” field of the draft certification criteria along with the relevant recitals of the GDPR.
22. In addition to the assessment mentioned in criterion II-a-18, the entity should also substantiate the choice made regarding the data transfer mechanism, pursuant to Chapter V of the GDPR.⁷ Therefore, the Board recommends that the LU SA takes into account in the draft criteria the need to substantiate the choice made with respect to the data transfer mechanism.

2.6 Principles of Article 5

23. Regarding the purpose of compatibility under section II-b-2, the Board recommends the LU SA to add more details in relation to the elements on which the compatibility assessment of further purposes must be based, at least the ones established by Article 6(4) of the GDPR, as the criteria for the compatibility test listed therein are missing. Regarding section II-c-1, the Board encourages the LU SA to take into account the amount, type and nature of the data collected and processed among the factors to consider as likely to influence the implementation of the principle of data minimisation.
24. With regard to section II-c-2 “, the Board encourages the LU SA to clarify in the context of “less intrusive means” what needs to be demonstrated.
25. Regarding the principle of data accuracy in section II-d-2, the draft certification criteria state that “The entity has defined and implemented a procedure to verify on a regular basis and at least annually the personal data it received, either by directly contacting the data subject, or by contacting the source from which it received the data. The entity documents this verification of data accuracy and has implemented a procedure to update data if necessary” The Board encourages the LU SA not to limit the personal data referred to in these criteria to the ones the entity “received”, but also refer to the data it holds in general (e.g. those inferred or created from the data received or otherwise produced by the entity). Furthermore, for reasons of completeness, in the passage “to update data if necessary”, the Board encourages the LU SA to add that data will also be corrected or deleted where necessary.
26. Regarding the deletion or anonymisation of data in section II-e-2, the draft certification criteria list certain use cases in which the applicant is required to effectively ensure these operations. In particular, the second and third bullet point mention: “where personal data is not, or no longer necessary for the purpose of the processing; when it no longer needs the data; or”. The Board notes that another use case might be where the SA orders the erasure of personal data under Article 58(2)(g) of the GDPR. In any case, the Board encourages the LU SA to clarify the difference between the two use cases described in these two bullet points or otherwise delete one of them, as well as to take into account in the draft certification criteria other possible use cases, such as the one of Article 58(2)(g).

2.7 General Obligations for Controllers and Processors

⁷ In the context of this assessment, the relevant CJEU judgements and the EDPB Guidelines and recommendations should be taken into account.

2.7.1. Obligation applicable to controllers and processor

27. Under section I-11 of the draft certification criteria, regarding the DPO's competences, the Board notes that if the DPO does not have minimum three years of professional experience, he/she either (i) "needs to have two years of legal experience and has followed comprehensive trainings on data protection" or (ii) "The DPO has access to legal assistance internally, or via a non-limiting service contract with an external firm, covering all GDPR subjects". The Board is of the opinion that the second requirement should not stand alone for the assessment of the DPO's qualification. This means that the DPO should not be considered qualified only because he/she "has access to legal assistance internally, or via a non-limiting service contract with an external firm, covering all GDPR subjects". This could be an additional requirement for the evaluation of DPO's qualifications, but not a stand-alone one. Since the scheme heavily relies on the DPO, it is important that he/she has the appropriate expertise. In addition, the required trainings on data protection should be recent and up to date. Therefore, the Board recommends that the LU SA amends this section accordingly.
28. Under section I-12 of the draft criteria (last point) the LU SA refers to cases where conflicts of interest of the DPO have been identified. The Board welcomes this inclusion, it however considers that the notification to the entity's highest management and the documentation of the conflicts of interest are not enough. It is essential that this conflict of interest is resolved according to an established procedure. Therefore, the Board recommends the LU SA to add this element under this section.
29. The Board notes that, under section I-13 of the draft criteria, the LU SA refers to the obligation of the DPO to "inform and advise the entity and its employees, who carry out processing activities, of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions [...]". The LU SA clarified that this does not refer to data protection provisions of other Member States, but to provisions of national laws and regulations. Therefore, the Board encourages the LU SA to modify this reference accordingly in the criteria.
30. The Board notes that sections I-14 and I-15 of the draft certification criteria are devoted to data breaches: the first one is designed to be applicable to controllers and the second one to processors. In particular, these sections require the implementation of "technical and organisational measures to identify, manage and notify personal data breaches" by the entity seeking for certification. Those measures have to cover various aspects, including the degree of involvement of the DPO. However, in this regard, both criteria seem to be contradictory as, on the one hand, they require that "the DPO should always be informed of each data breach", while, on the other hand, they refer to a "formal procedure" in place defining "when the DPO needs to be informed and what this information shall include". Indeed, it is not clear if these two requirements refer to different factual contexts. Therefore, the Board recommends the LU SA to explain if it this is the case and to solve this contradiction between both sections anyhow.
31. In section I-14, with regard to the notification to the SA, the Board recommends the LU SA to delete the term "if applicable" from the sixth bullet point.
32. Section I-15 of the draft certification criteria, which applies to processors, envisages the implementation of "technical and organisational measures to detect, manage and notify personal data breaches towards the contractual partner(s) and / or controller(s) within a timeframe allowing the controller to notify the supervisory authority within 72 hours". With

regard to the envisaged timing, the Board notes that Article 33(2) of the GDPR requires the processor to notify the personal data breaches to the controller “without undue delay” after becoming aware of it. Therefore, the Board recommends the LU SA to add the term “without undue delay” in relation to the processor’s obligation to this section.

2.7.2. Obligations applicable to the controllers

33. The Board notes that section II-f-7 mentions that “The entity reviews the DPIA on a regular basis and at least annually or when significant changes impacting the DPIA occur. The entity takes into account the formal opinion of its DPO”. The Board recommends the LU SA to bring this section in line with Article 35(9) of the GDPR, so as to consider the opportunity to seek the views of data subjects or their representatives (without prejudice to the protection of commercial or public interests or the security of processing operations).
34. In relation to the DPIA review in section II-f-7, it is mentioned that this shall be carried out, among others, “when significant changes impacting the DPIA occur”. In this regard, the criterion requires the entity to implement “a documented method ensuring that it took into account all factors likely to influence the DPIA” and that “such factors can be external or internal and include among others changes in the applicable regulatory framework [...].” In relation to those changes, the Board recommends the LU SA to also add a reference to changes of the risk represented by processing operations as envisaged by Article 35(11) of the GDPR.
35. Regarding section II-f-9 of the draft certification criteria, titled “assessment of sufficiency” which concerns the use of processors by the applicant, the Board encourages the LU SA to take into account the expert knowledge, reliability and resources that the processor needs to have before engaging it, in line with Recital 81 of the GDPR. Furthermore, with regard to the last bulled point of this section, the Board recommends the LU SA to make clear that the audits the controller is required to perform, according to sections II-f-5 and II-f-6 of the draft certification criteria, can be conducted towards the processor.
36. In section II-f-10 regarding a contract / legal act under Union or Member State law, the Board recommends the LU SA to include a reference to the elements that must be set out in this contract/legal act under Article 28(3) of the GDPR, such as 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.
37. Moreover, when the draft certification criteria mention that there has to be a contract / legal act under Union or Member State law in place, the Board recommends to specify that, according to Article 28(9) of the GDPR, this should be in writing (including in electronic form) so to be checked by the certification body.
38. With regard to the sixth bullet point of the same criteria, stating: “The processor assists the entity in ensuring compliance with his obligations taking into account the nature of processing and the information available to the processor”, the Board encourages to add a reference to the entity’s legal obligations which result from Articles 32 to 36 of the GDPR.
39. The criteria in section II-f-12 refer to “due diligences procedures” in addition to audit and monitoring by the applicant towards the engaged processors. The Board notes that the term “due diligence” can be very broad and take on different meanings, depending on the content and structure of the underlying contract, which in turn places special data protection

requirements on the respective audits. Therefore, since the risk of non-compliant implementation is not insignificant and the use of this term can lead to ambiguity about the necessary extent of audits, the Board encourages the LU SA to clarify the term “due diligence procedure” in the draft criteria.

2.7.3. Obligations applicable to processors

40. With regard to Section III of the draft certification criteria, concerning the principles relating to processing of personal data by the processor or the sub-processor, the Board recommends the LU SA to add in section III-1 that the contract or legal act between processor and controller or sub-processor and processor should be in writing (including in electronic form) in line with Article 28(9) of the GDPR.
41. When the same draft certification criteria mention that the entity “assists the contractual partner and the controller in ensuring compliance with his obligations taking into account the nature of processing and the information available to the entity, the Board encourages the LU SA to add an explicit reference to the sub-processor’s obligations to assist the processor and the similar obligation of the processor to assist the controller with regard to the obligations of the latter under Articles 32-36 of the GDPR.
42. With regard to section III-3 of the draft criteria, concerning the limitation of the processing to the documented instructions received by the controller or the contractual partner, the Board recommends the LU SA to add a reference to international transfers in line with Article 28(3)(a) of the GDPR.
43. Under section III-11 of the draft certification criteria regarding the assessment of sufficiency, the Board notes that there should be a reference to the processor’s obligation to assess the sub-processors it intends to engage.⁸ The Board encourages the LU SA to modify this criterion accordingly.
44. With regard to section III-3 of the draft certification criteria concerning the transfer of personal data to third countries, the Board recommends to adjust this criterion to the recommendation set out above as regards section II-a-18.

2.8 Rights of data subjects

45. Under section I-9 of the draft certification criteria “facilitate the exercise of data subjects’ rights”, the Board takes note of two different scenarios of impossibility of the entity to comply with the request set by controller. The Board understands that the first scenario refers to situations that the entity cannot comply within the deadline set by the controller, while the second refers to an absolute impossibility to comply. However, the distinction between the two scenarios is not clear in the criteria, thus the Board encourages the LU SA to clarify this.
46. With respect to the exercise of the data subject rights, the Board welcomes, in relation to the fees that can be charged by the controller, in case of manifestly unfounded or excessive requests from the data subject, the obligation of the entity to document “how it justifies the amount of the charged fees”. This obligation is found in section II-a-10 (right to object) section

⁸ Similar obligations are provided in the EDPB Opinion on Article 28 GDPR SCCs, clause 7.6. regarding the authorisation to use a sub-processor “In order to make the assessment and the decision whether to authorise sub-contracting, the data processor shall provide the data controller with all necessary information on the intended sub-processor, including on their locations, the processing activities they will be carrying out and on any safeguards and measures to be implemented.”

II-a-11 (right to restriction of the processing), section II-a-12 (right not to be subject to automated individual decision-making), section II-a-16 (right to access) and section II-a-17 (right to data portability). In this regard, the Board notes that the elements to take into account to consider reasonable the amount of the charged fees are specified in Article 12(5)(a) of the GDPR and should not be left to the discretion of the entity seeking for certification or the certification body. Therefore, the Board recommends the LU SA to include a reference to these elements in this section (i.e. the administrative cost of providing the communication or taking the action requested by the data subject).

47. As regards the right of data subject not to be subject to automated decision-making including profiling, the Board notes that “profiling” is included in the title of the relevant Section, II-a-12. However, it is missing from the main text of the criterion (first paragraph). The Board encourages this addition.
48. Moreover, data subjects’ right of access is provided under section II-a-16 of the draft certification criteria. However, the draft misses to include the list of information to be provided to the data subject, pursuant to Article 15(1). Therefore, the Board encourages, for consistency with the rest of the draft certification criteria devoted to data subjects’ rights, to also refer here to all the obligations provided under Article 15(1) of the GDPR (i.e. the information that the controller should provide to data subjects when they exercise their right of access).
49. Within the same Section, the Board notes that the draft certification criteria do not include that the first time the entity provides a copy to the data subject, this should be free of charge and that for any further copies requested, the entity may charge reasonable fees based on administrative costs. The Board recommends that the LU SA includes this aspect in the criteria.
50. Similarly, the reference to the modalities on how to provide the information requested by the data subject, is missing. The Board recommends to add a clarification thereof that when the data subject makes the request by electronic means, and unless otherwise requested, the information must be provided in a commonly used electronic form.
51. Under the section II-a-17 regarding the right to data portability, an important element to be assessed is missing. In particular, pursuant to Article 20(4) of the GDPR, there is need to assess whether the data subjects’ right to data portability adversely affects the rights and freedoms of others. The Board recommends this addition, as this element also need to be assessed by the certification body in the context of the right to data portability.

2.9 Risks for the rights and freedoms of natural persons and technical and organisational measures guaranteeing protection

52. Regarding the sections about the risk analysis, in II-f-2 and III-6 it is not made clear enough which risks are being addressed, namely those of the data subjects. The Board recommends the LU SA to include, among the risks mentioned in this requirement, those to the rights and freedoms of the data subjects. In addition, the Board recommends that the LU SA adds more information regarding the different types of risks with regard to the data subjects concerned.

53. In line with the previous recommendations concerning the risk analysis, the Board recommends the LU SA to also add, in section II-f-3 and III-7, that the risk treatment takes into account the different types of risks to the rights and freedoms of the data subjects concerned.
54. Furthermore, it is mentioned that the entity should consider at least the technical and organisational measures of the access control policy. The Board recommends the LU SA to bring this in line with Article 32(4) of the GDPR by adding the entity's obligation to take steps to ensure that any natural or legal person acting under its authority, who has access to personal data, does not process them except on instructions from the entity, unless he or she is required to do so under Union or Member State law.
55. The draft certification criteria also state in II-f-3 and III-7 that the entity reviews the effectiveness of the risk treatment plan at least on an annual basis or when changes impacting the risk evaluation occur and adapts the risk treatment plan if necessary. The Board encourages the LU SA to make clear that there are processes in place to measure and ensure the effectiveness of the said plan, so as to ensure that the certification criteria are self-explanatory and that the certification body could know what it needs to check from the sole formulation of the criteria.
56. Regarding the implementation of organisational and technical measures the draft certification criteria state in section II-f-4 and III-8 that on a daily basis, reports on controls performed and security incidents related to the processing activities in scope shall be provided at least to the DPO and the entity's management. The Board encourages the LU SA to add that these reports should be provided also to the relevant persons within the organisation who are involved - so not only to the DPO and the entity's management.

3 CONCLUSIONS / RECOMMENDATIONS

57. By way of conclusion, the EDPB considers that the GDPR – CARPA certification criteria may lead to an inconsistent application of the GDPR and the following changes need to be made in order to fulfill the requirements imposed by Article 42 of the GDPR in light of the Guidelines and the Addendum:
58. regarding the “scope of the certification mechanism and target of evaluation (TOE)”, the Board recommends that the LU SA:
- 1) includes specific criteria covering processing activities under Articles 85 to 89 of the GDPR.
 - 2) includes an analysis of the relevant laws which shall be performed by the entity demonstrating that specific and suitable measures have been put in place in order to respect the fundamental rights and interests of data subjects pursuant to Article 89 of the GDPR
59. regarding the “procedure to determine a target of evaluation (TOE)” the Board recommends that the LU SA:
- 1) includes in the beginning of the draft certification criteria, in a devoted section, sufficient information with regard to the criteria on how the ToE is defined .
60. regarding the “certification criteria” the Board recommends that the LU SA:

1) amends the criteria listed in paragraph 10 of this Opinion by providing the factors that shall be taken into account by the applicant when carrying out the relevant assessments so as to also clarify what will be checked by the certification body.

61. regarding the “lawfulness of the processing” the Board recommends that the LU SA:

1) modifies section II-a-1 which refers to a “valid legal basis” so as to take into account how the applicability of the legal basis is demonstrated and its appropriateness, where relevant, considering the processing activities, depending on the nature, context, scope and purposes of the processing.

2) in relation to section II-a-3, takes into account that the entity demonstrates the “appropriateness” of consent as legal ground for the processing in the individual case, so to have this criterion in line with Recital 43 of the GDPR and the 05/2020 EDPB Guidelines on consent under the GDPR.

3) in section II-a-3 adds, the minimum requirements which have to necessarily be met so that consent can be considered informed and unambiguous and that the certification criteria bring sufficient added value for the GDPR compliance of the certified entities.

4) takes into account, where necessary, throughout section II-a-9, the appropriate safeguards, as provided by Article 9(2) of the GDPR with regard to the processing of special categories of data, and modify the related criteria accordingly .

5) modifies the criterion under section II-a-9 which refers to Article 9(2)(b) of the GDPR, so as to take into account that the controller must be authorised for such processing by Union or Member State law or a collective agreement pursuant to the Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject, in order to allow the certification’s body assessment to be exhaustive.

(6), takes into consideration, in section II-a-9, the appropriate safeguards, as provided in Article 9(2)(d) of the GDPR regarding the “legitimate activities by a foundation, association or any other non-for-profit body [...].

(7) takes into account, in section II-a-9, the specific measures taken to safeguard the fundamental rights and interests of the data subject with regards to the “substantial public interest” in the context of Article 9(2)(g) of the GDPR.

(8) modifies, in section II-a-9, the criterion so as to refer to the further conditions, including limitations regarding the processing of genetic, biometric and data regarding health, set out in national law pursuant to Article 9(4) of the GDPR, where relevant.

(9) includes a reference to Article 44-45 of the GDPR in the “Label” field of section II-a-18 of the draft certification criteria along with the relevant recitals of the GDPR.

(11) requires, in section II-a-18, that the entity substantiate the choice made with regard to the data transfer mechanisms, pursuant to Chapter V of the GDPR.

62. regarding the “principles of Article 5” the Board recommends that the LU SA:

(1) adds, under section II-b-2, more details in relation to the elements on which the compatibility assessment of further purposes must be based, at least the ones established by Article 6(4) of the GDPR.

63. regarding the “general obligations for controllers and processors” the Board recommends that the LU SA:

(1) modifies the criterion under section I-11, regarding the DPO competences, so to make sure that the (ii) requirement does not stand alone, but is an additional requirement for the assessment of the DPO’s qualification and that the required trainings on data protection are recent and up to date.

(2) adds, under section I-12, that when a conflict of interest has been identified, it will be resolved according to an established procedure.

(3) clarifies, in sections I-14 and I-15, the degree of DPO’s involvement when, on the one hand, the draft criteria require that “the DPO should always be informed of each data breach”, while, on the other hand, they refer to a “formal procedure” in place defining “when the DPO needs to be informed and what this information shall include”.

(4) deletes the term “if applicable” from the sixth bullet point of section I-14 with regard to the notification of data breaches to the SA .

(5) adds to section I-15 the term “without undue delay” in relation to the processor’s obligation to notify the personal data breach to the controller” after becoming aware of it, pursuant to Article 33(2) of the GDPR.

(6) modifies, in relation to the DPIA review, section II-f-7 to bring it line with Article 35(9) of the GDPR, so as to consider the opportunity to seek the views of data subjects or their representatives (without prejudice to the protection of commercial or public interests or the security of processing operations).

(7) modifies, with regards to factors likely to influence the DPIA, section II-f-7 to include a reference to the changes of the risk represented by processing operations envisaged by Article 35(11) of the GDPR.

(8) modifies the last bullet point of section II-f-9, to make clear that the audits that the controller is required to perform according to the sections II-f-5 and II-f-6 of the draft certification criteria can be conducted towards a processor.

(9) adds, under section II-f-10, a reference to the elements that must be set out in the contract/legal act under Article 28(3) of the GDPR, such as 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.

(10) specifies, under section II-f-10 and III-1, that when there has to be a contract/legal act under Union or Member State law in place, according to Article 28(9) of the GDPR, this should be in writing so as to be checked by the certification body.

(11) under section III-3, regarding the limitation of the processing to the documented instructions received by the controller or the contractual partner, includes a reference to international transfers in line with Article 28(3)(a) of the GDPR.

(12) adjusts section III-3 of the draft certification criteria to the recommendation provided for section II-a-18.

64. regarding the “rights of data subjects” the Board recommends that the LU SA:

(1) includes a reference to the elements to be taken into account to consider the reasonable amount of charged fees provided in Article 12(5)(a) of the GDPR in case of manifestly unfounded or excessive requests from the data subject (i.e. the administrative cost of providing the communication or taking the action requested by the data subject).

(2) includes, under section II-a-16, that the first time the entity provides a copy to the data subject, this should be free of charge and that for any further copies, the entity may charge reasonable fee based on administrative costs.

(3) clarifies in the same section that when the data subject makes the request by electronic means, and unless otherwise requested, the information must be provided in a commonly used electronic form.

(4) includes in section II-a-17 that there is need to assess whether the data subjects' right to data portability adversely affects the rights and freedoms of others.

65. regarding the "risks for the rights and freedoms of natural persons" and the "technical and organisational measures guaranteeing protection" the Board recommends that the LU SA:

(1) includes, among the risks mentioned in sections II-f-2 and III-6, those to the rights and freedoms of the data subjects and adds information regarding the different types of risks with respect to the data subjects concerned.

(2) adds, under sections II-f-3 and III-7, that the risk treatment takes into account the different types of risks to the rights and freedoms of the data subjects concerned.

(3) aligns the requirement of the entity to consider at least the technical and organisational measures of the access control policy with Article 32(4) of the GDPR by adding the relevant obligation.

66. Finally, in line with the Guidelines the EDPB also recalls that, in case of amendments of the GDPR-CARPA certification criteria involving substantial changes⁹, the LU SA will have to submit the modified version to the EDPB in accordance with Articles 42(5) and 43(2)(b) of the GDPR.

4 FINAL REMARKS

67. This Opinion is addressed to the LU SA and will be made public pursuant to Article 64(5)(b) of the GDPR.

68. According to Article 64(7) and (8) of the GDPR, the LU SA shall communicate its response to this Opinion 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.

⁹ See section 9 of the Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation providing "Guidance on certification criteria assessment" for which the public consultation period expired on 26 May 2021.

69. Pursuant to Article 70(1)(y) GDPR, the LU SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
70. The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the LU SA shall make public the GDPR-CARPA certification criteria in an easily accessible form, and transmit them to the Board for inclusion in the public register of certification mechanisms and data protection seals, as per Article 42(8) of the GDPR.

For the European Data Protection Board
The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 70.I.b)

Art.70.I.b

Opinion 20/2021 on Tobacco Traceability System

Adopted on 18 June 2021

Contents

1. BACKGROUND	3
2. SCOPE OF THE OPINION	4
3. ASSESSMENT.....	5

The European Data Protection Board

Having regard to Article 70(1)(b) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

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

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

HAS ADOPTED THE FOLLOWING OPINION:

1. BACKGROUND

1. On 3 March 2021, the European Commission (“Commission”) requested the opinion of the EDPB, on the basis of Article 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 of the European Parliament and of the Council of 3 April 2014 on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC (the “Tobacco Products Directive” or “Directive”).
2. The Tobacco Products Directive envisages the establishment of a traceability system to track and trace the movements of tobacco products within the Union territory, in order to facilitate the smooth functioning of the internal market for tobacco and related products and ensure their compliance with the Directive.² On the basis of Article 15(11) Directive, the Commission adopted the Commission Implementing Regulation (EU) 2018/574 and Commission Delegated Regulation (EU) 2018/573 which lay down, respectively, technical standards for the establishment and operation of a traceability system for tobacco products and the key elements of data storage contracts to be concluded as part of a traceability system for tobacco products.
3. Under the tobacco traceability system, all unit packets of tobacco products are required to be marked with a unique identifier. The ID Issuers are the actors entrusted with generating and issuing the unique identifier. Personal data processed in this context are related to the request of the unique identifier code for economic operators (e.g. contact details, VAT number, address of economic operators that are natural persons or whose information relate to natural persons).³ The information collected by the ID Issuers (including personal data) is stored in the ID Issuers’ registries and transmitted to the secondary repository, which is part of the repositories system, composed by the primary repositories,

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

² Articles 1 and 15 Directive.

³ See CJEU Joined Cases C-92/09 and C-93/09, with regard to the protection of the personal data of natural persons who are identified or identifiable on the names of legal persons.

- the secondary repository and a routing service (“the router”) set up and managed by the provider of the secondary repository.
4. The providers of primary repositories are contracted by the tobacco manufacturers and importers and approved by the Commission. These host information (including personal data) relating to tobacco products of the manufacturer or importers who contracted the repository. The information is shared with the secondary repository, which is a central data storage repository containing a copy of all the data stored in the primary repositories and ID Issuers registries. Personal data processed in this context relate to recording and transmitting information on product movements or transactional information (e.g. contact details of destination facilities of sole traders; contact details and VAT numbers of buyers and payers who are sole traders or whose name may identify a natural person).
 5. The competent authorities of the Member States and the Commission have access to the data stored in the primary and secondary repositories and are entrusted with enforcement and monitoring tasks, respectively, to ensure compliance with the Directive and relevant legislation.

2. SCOPE OF THE OPINION

6. The Commission requested the opinion of the EDPB, on the basis of Article 70(1)(b) GDPR, on the data protection aspects of the tobacco traceability system. The Commission asked, in particular, three specific questions:
 - I. Does the European Data Protection Board agree with the Commission’s assessment according to which the Member States and the Commission act as joint controllers with regard to the processing of personal data in the context of the EU tobacco traceability system, as explained in the background information in this note?
 - II. Does the European Data Protection Board agree with the Commission’s assessment according to which the ID Issuers act as processors of the Member States as explained in the background information in this note?
 - III. Does the European Data Protection Board agree with the 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 processor on behalf of the joint controllers (Commission and Member States), as explained in the background information in this note?
7. The EDPB would like to underline that, in accordance to art. 70(1)(b) of the GDPR, the EDPB is tasked with providing advice to the Commission on any issue related to the protection of personal data in the Union. This task, however, should not be understood as an obligation of the EDPB to advise the Commission with regard to specific processing operations where the latter is involved as a controller or processor. In this regard, the EDPB recalls that the responsibility to ensure compliance with the applicable data protection legislation, including the assessment of the role of the actors involved in the processing activities at stake, lies with the controller and processor, assisted by, where applicable, their data protection officer. In the spirit of the principle of cooperation that governs the inter-institutional at an EU level relationship between the Commission and the EDPB, the present Opinion contains elements to be considered by the Commission. It is made only on the basis of the Commission’s assessment as provided to the EDPB. This Opinion has the nature of a general advice and does not, in

- any manner, intend to provide definitive views and legal analysis as it does not substitute the obligations of the controller(s) to ensure that the processing of personal data is compliant with the applicable data protection legislation, including with regard to the determination of the roles of the actors involved. In addition, the omission of any references, in this opinion, to any other aspects of the processing of personal data within the system does not signal either approval or disapproval from the EDPB or any of its members, as data protection regulators. This is without prejudice to any specific further assessments conducted by the European Data Protection Supervisor (“EDPS”) or the national data protection Supervisory Authorities.
8. Moreover, the EDPS remains the entity responsible for the supervision of EU institutions, bodies, offices and agencies regarding the processing of personal data in the context of their mandates, as foreseen in Regulation 2018/1725.⁴ As a result, any requests from the Commission concerning compliance with, or implementation of any provisions regarding Regulation 2018/1725 should be addressed primarily to the EDPS.
 9. Finally, the EDPB also recalls that in line with the GDPR, the national data protection supervisory authorities remain entirely responsible for the supervision of the processing of personal data within the tobacco traceability system by the national authorities and economic operators in their Member States. The EDPS and the national authorities are regularly making available guidelines and practical tools to assist Controllers and Processors to ensure data protection compliance.
 10. The EDPB also invites the Commission to consider the published EDPB guidelines aiming to ensure consistent application of the GDPR.

3. ASSESSMENT

(1) Does the European Data Protection Board agree with the Commission’s assessment according to which the Member States and the Commission act as joint controllers with regard to the processing of personal data in the context of the EU tobacco traceability system, as explained in the background information in this note?

11. In accordance with article 26 GDPR “[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers”. As underlined in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (the “Guidelines”), “jointly” means “together with” or “not alone” and the assessment of joint controllership entails the factual analysis of the actual influence on the determination of the purposes and means of the processing.⁵ In this regard, an important criterion to identify the joint determination is “whether the processing would not be possible without both parties’ participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.”⁶
12. In the present case, the EDPB understands that the purposes of the processing stem from Directive 2014/40/EU. With the objective to facilitate the smooth functioning of the internal market for tobacco

⁴ See article 52 of Regulation 2018/1725.

⁵ Par. 48 and 49 Guidelines.

⁶ Guidelines par. 53.

and related products and ensure compliance with the provisions of the Directive,⁷ Article 15 Directive envisages the establishment of a tobacco traceability system to track and trace the movements of tobacco products within the EU. Under this system, all unit packets of tobacco products are marked with a unique identifier. This allows the tracking and tracing of the tobacco packets, since economic operators involved in tobacco trade are required to record the relevant information throughout the supply chain. The data collected (including personal data) are made accessible to the Commission and Member States. The latter are entrusted with ensuring the compliance of tobacco and related products with the Directive and the implementing and delegated acts provided for therein, including by laying down rules on penalties applicable to infringements and ensuring that the penalties are enforced.⁸ The Commission is entrusted with monitoring tasks.⁹ The respective duties and powers of the Commission and the Member States are described in the Implementing Regulation 2018/574.

Joint determination of the purposes

13. As underlined in the Guidelines, a joint determination of the purpose exists when the entities involved process the data for the same, or common, purposes or for purposes, which are closely linked or complementary.¹⁰
14. In general terms, it is the EDPB's understanding that the processing of personal data in the context of the tobacco traceability system takes place for tobacco control purposes, in order to ensure compliance with the Directive and relevant legislation, as explained above. As laid out in the Directive, both the Commission and the Member States are entrusted with monitoring and enforcement tasks, respectively, these tasks being complementary and inextricably linked.¹¹ Consequently, it appears that the Directive provides the relevant elements to assess whether the Member States and the Commission share the common purpose to ensure compliance with the Directive and with the relevant legislation.
15. As stated above, joint controllership exists when the different parties determine jointly the purpose and the means of the processing activity. Thus, assessing the existence of joint controllers requires not only examining whether the purposes are determined by more than one party, but also the means.¹²

Joint determination of means

16. As stated in the Guidelines, the joint determination of the means of the processing does not entail that each entity needs in all cases to determine all of the means. Thus, "*different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so*".¹³

⁷ See Article 1 Directive.

⁸ See article 23(2) and 23(3) Directive.

⁹ See, for example, article 15.8 of the Directive that entrusts the Commission with ensuring the suitability, in particular its independence and technical capacities, of the primary repository providers and with approving the external auditor tasked to monitor the activities of the primary repository providers.

¹⁰ Pars. 57-58 Guidelines.

¹¹ See, for example, Art. 25(1)(l), 26(6), 27(2), 27(3)(a), 27(4) and 27(5) Regulation 2018/574 provides the Commission and the Member States with the same tasks.

¹² Guidelines, para. 48.

¹³ Guidelines, para. 61.

17. Within the tobacco traceability system, there are two types of locations in which personal data are processed, by means of storage and exchange: the registries established and maintained by the ID issuers and the repositories system (which include the primary repositories, the secondary repository and the router set up and managed by the provider of the secondary repository). Personal data are processed through those different platforms, which are necessary for the functioning of the tobacco traceability system. Without the mediation of the ID issuers and the repositories, data (including personal data) would not be collected, exchanged and made accessible to the Member States and the Commission.
18. As stated in the Guidelines, “[e]ssential means’ are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller”.¹⁴ Given the specific functioning of the tobacco traceability system as described in the Directive and Regulation 2018/574, it appears that the purpose of ensuring compliance with the Directive and relevant legislation would not be attainable without the involvement of the ID issuers and the providers of the repositories, which provide the platforms that allow the collection, storage and exchange of information.¹⁵
19. According to Article 3 of Commission Implementing Regulation 2018/574, the ID issuers that establish and maintain the first type of registries are entities appointed by the Member States. In addition, Member States are entrusted with ensuring that the ID issuers comply with the independence requirements laid down in Article 35 of Regulation 2018/574. The Commission is not directly involved in the choice of the ID issuers. However, it is tasked with the monitoring of the compliance of the ID issuers with the independence requirements.¹⁶ The information gathered in the ID issuers’ registries is forwarded to the secondary repository via the router, where it can be accessed by the Commission and the competent authorities of the Member States.
20. The secondary repository contains a copy of all data stored in the different primary repositories and ID Issuers’ registries, as per Articles 20(3) and 27(1) Regulation 2018/574. Member States and the Commission have access to the data stored in the primary and secondary repositories, and have the right to create, manage and withdraw user access rights for the repositories and to download full and selected sets of data for the purposes foreseen in the Directive.¹⁷ The provider of the secondary repository, who is also in charge of providing the router, is appointed by the Commission from among the providers of primary repositories.¹⁸ Likewise, the Commission is entrusted to approve the provider of the primary repository proposed by the manufacturer or importer, as well as the draft storage contract.¹⁹ Member States do not have any influence on the choice, but they are entrusted with ensuring that manufacturers and importers conclude data storage contracts with providers of primary repositories.²⁰ In addition, Member States shall monitor and ensure the compliance of the providers of the primary repositories with the independence requirements.²¹

¹⁴ Guidelines, para. 38.

¹⁵ See Art. 1(b) Directive, which refers to the traceability of tobacco products “to ensure their compliance with [the] Directive”. Article 15 Directive provides for the key elements of the tobacco traceability system.

¹⁶ See art. 35.4 and 35.7 of Regulation 2018/574.

¹⁷ See article 25(1)(k)-(l) and 25(2) of Regulation 2018/574.

¹⁸ See Article 27(1) and Annex I Part B par. 1 to Implementing Regulation 2018/574.

¹⁹ See Article 15(8) Directive and Annex I Part A par. 3 to Implementing Regulation 2018/574.

²⁰ Article 15(8) Directive.

²¹ Article 35(6) Regulation 2018/574.

21. From the above, it seems to be apparent that, whereas Member States exert a decisive influence on the choice of the ID Issuers, the Commission does so with regard to the providers of the repositories, by approving the proposed providers of primary repositories and appointing the provider of the secondary repository. In this context, it is relevant to underline that, as stated in the Guidelines, “[p]rocessing of personal data can involve multiple processors. For example, a controller [or joint controllers] may itself choose to directly engage multiple processors, by involving different processors at separate stages of the processing (multiple processors).”²²
22. In the present case, all the means used for the processing of personal data are necessary in order to achieve the purpose of ensuring compliance with the Directive and relevant legislation. In fact, whereas all the data are eventually stored in the secondary repository, the traceability of the tobacco products would not be possible without the information provided by the ID Issuers (and the primary repositories). In other words, in order to achieve the purpose of monitoring compliance with and enforcing the rules in the context of the tobacco traceability system, all the means identified (i.e. the ID Issuers’ registries and the repositories) are necessary. Otherwise, the traceability of the tobacco products would not be possible and, therefore, the purpose of the processing would not be achievable.
23. In light of the elements above and as a preliminary analysis, the EDPB considers **that the Commission has taken into consideration the necessary elements to perform the assessment of joint controllership. This is 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 supervisory authority in the exercise of its powers.**
24. In addition, the EDPB recalls that the existence of joint controllership does not necessarily imply equal responsibility of the different actors involved.²³ The level of responsibility shall be assessed on a case-by-case basis, taking into account the specific circumstances of the case. In this regard, the EDPB recalls that joint controllers “can have a certain degree of flexibility in distributing and allocating obligations among them as long as they ensure full compliance with the GDPR with respect of the given processing. The allocation should take into account factors such as, who is competent and in a position to effectively ensure data subject’s rights as well as to comply with the relevant obligations under the GDPR”.²⁴

(2) Does the European Data Protection Board agree with the Commission’s assessment according to which the ID Issuers act as processors of the Member States as explained in the background information in this note?

25. In the background information provided by the Commission, it is stated that, since the Commission is not involved in the establishment and functioning of the ID Issuers and the processing is based on their contractual relationship with the Member State that appoints them, the ID Issuers do not qualify as the Commission’s processor.
26. The EDPB recalls that there are two basic conditions to qualify as a processor: being a separate entity in relation to the controller and processing personal data on the controller’s behalf.²⁵ As the EDPB has previously stated, processing personal data on the controller’s behalf requires that the separate entity

²² Guidelines, para. 73.

²³ See Guidelines para. 56.

²⁴ See Guidelines para 165.

²⁵ Guidelines, para. 74.

process personal data for the benefit of the controller. This entails that the processors implement the instructions given by the controller with regard to the purpose of the processing and the essential elements of the means.²⁶

27. In the case of the ID Issuers, albeit some of the elements of the processing may be laid down in the contracts between the ID Issuers and the Member State appointing them, other relevant aspects of the processing, in particular regarding the exchange with the secondary repository, seem to be determined otherwise, as explained in the next paragraphs.
28. As indicated above, the role of the ID Issuers within the tobacco traceability system is to generate and issue unique identifiers and transmit the information (including the personal data collected in the context of generating and issuing the unique identifier) to the secondary repository via the router.²⁷ Once the information is transmitted to the secondary repository, the Commission and the Member States can access it for the purpose of ensuring compliance. The transmission of the data to the secondary repository via the router takes places "*using the data format and data exchange modalities defined by the router*"²⁸, which is set up and managed by the secondary repository provider.²⁹ In addition, it shall be noted that, as per Article 28(1) Regulation 2018/574, "[t]he provider operating the secondary repository shall communicate to providers operating primary repositories, ID issuers and economic operators, the list of specifications required for the data exchange with the secondary repository and the router. All specifications shall be based on non-proprietary open standards".
29. From the above, it appears that the ID Issuers shall follow the provisions of Regulation 2018/574 (including the technical specifications in its Annex) and the instructions of the secondary repository provider with regard to the storage and especially the exchange of data -including personal data, within the tobacco traceability system. In addition, it stems from the Directive that the processing of personal data by the ID Issuers is necessary in order to ensure compliance with the Directive and the relevant legislation, which would not be possible without the data transmitted by the ID Issuers.³⁰
30. In light of the elements above and as a preliminary analysis, the EDPB considers **that the 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. This is 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 supervisory authority in the exercise of its powers.**
31. As underlined above, the joint controllership arrangement shall include the distribution of the responsibilities, taking into account the specific circumstances of the case. In this respect, as stated in

²⁶ Guidelines, para. 78.

²⁷ Articles 3 and 20(3) Regulation 2018/574.

²⁸ Article 29(3) Regulation 2018/574.

²⁹ Article 24(1)(c) Regulation 2018/574.

³⁰ In this regard, Article 15(1) Directive states that: "Member States shall ensure that all unit packets of tobacco products are marked with a unique identifier".

the Guidelines, the use of a processor is one of the elements to be considered by the joint controllers when determining their respective responsibilities.³¹

(3) Does the European Data Protection Board agree with the 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 processor on behalf of the joint controllers (Commission and Member States), as explained in the background information in this note?

32. The primary repositories, as defined under the EC implementing Regulation, are the repositories “*storing traceability data relating exclusively to the products of a given manufacturer or importer*”.³² In general, terms, as it is the case with the provider of the secondary repository and the ID Issuers, the primary repositories’ providers do not process personal data for their own purposes in this context. The data processed by the primary repositories’ providers within the tobacco traceability system facilitate the Commission and the Member States to ensure the effective monitoring and enforcement activities in the context of fighting illicit trade in tobacco products.
33. As explained above, each tobacco products’ manufacturer and importer is required to conclude a data storage contract with an independent third-party provider for establishing a primary repository. The key elements of the contract are established in the Commission Delegated Regulation 2018/573. The primary repositories host information, solely relating to the tobacco products of the manufacturer or importer that contracted such primary repository.³³ All the data received by the primary repository, in the context of a reporting activity, or for any other permitted reason shall be forwarded to the secondary repository the moment received.³⁴ In this regard, each primary repository shall enter into an individual contract with the provider appointed as a secondary repository to carry out their services.³⁵ In this context, and on the basis of clarifications provided by the Commission, the EDPB understands that the secondary repository provider also enters into a data processing agreement with the providers of the primary repositories, to ensure that the processing carried out by the latter is in accordance with Art. 28(2) and (3) of the GDPR.
34. Thus, it appears from the applicable legislation that the primary repositories are separate independent entities, in charge of storing and transmitting the received data to the secondary repository on behalf of a (joint) controller(s).
35. It shall be noted that, whereas in a given processing operation the essential means of the processing are determined by the (joint) controller(s), the decision on the non-essential means can be left to the processor. As stated in the Guidelines, non-essential means, “*concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures*”.³⁶ In the context of the tobacco traceability system, the Board notes that the specific rules

³¹ Guidelines, para. 163.

³² EC Implementing Regulation 18/574 Art. 2(13).

³³ EC Implementing Regulation 18/574 Art. 26(2).

³⁴ EC Implementing Regulation 18/574 Art. 26(2).

³⁵ EC Implementing Regulation 18/574 Annex I, Part B(4).

³⁶ See Guidelines, para. 38.

applicable to the processing carried out by the primary repositories are not determined by them nor they are specified in the contract with the manufacturer or importer.³⁷

36. The practical aspects of the implementation (or “non-essential means”) are set forth in Regulation 2018/574, in the service agreement signed with the secondary repository provider and in the technical instructions of the latter. In this regard, the storage of data (including personal data) in the primary repositories has to be conducted in accordance with the “common data dictionary” provided by the secondary repository,³⁸ which contains the technical aspects of the database kept by the primary and secondary repositories.³⁹ Likewise, when the primary repository conducts the transfer of data to the secondary repository, it is not independent in deciding the modalities of the transfer, but it should use the data format and data exchange modalities, as determined by the secondary repository.⁴⁰ Additionally, it seems that the secondary repository provider and the primary repositories’ providers also enter into a data processing agreement for the processing of personal data.
37. It stems from the above that the primary repositories act exclusively in accordance with the rules described in the Commission Implementing Regulation 2018/574, the technical instructions provided by the secondary repository and the contract with the operator of the secondary repository.
38. In light of the elements above and as a preliminary analysis, the EDPB considers **that the Commission has taken into consideration the necessary elements to perform the assessment on the role of the providers of the primary repository. This is without prejudice to any specific further assessment pursuant to relevant applicable data protection legislation carried out by the controller as part of its obligations or by a competent supervisory authority in the exercise of its powers.**
39. The EDPB underlines that the contract between a processor and a sub-processor shall include the same data protection obligations that apply to the processor with regard to the controllers.⁴¹
40. Finally, the EDPB recalls that, according to Art. 28(2) of the GDPR, in order to engage a (sub) processor, the processor needs the controller’s approval, either via prior specific or general written authorisation.

³⁷ Article 9 of Regulation 2018/573 only establishes the obligation to specify in the contract that the primary repository provider will put in place all appropriate measures to ensure the confidentiality, integrity and availability of the data stored and that it will be processed in accordance with the GDPR.

³⁸ EC Implementing Regulation 18/574 Art. 26(5).

³⁹ Article 2(17) Regulation 2018/574.

⁴⁰ EC Implementing Regulation 18/574 Art. 26(4).

⁴¹ Article 28(4) GDPR.

Barbara Scarafia
Vice-President
Amazon EU Sarl
38 Avenue John F. Kennedy
L-1855, Luxembourg City, Luxembourg

19 May 2020

Ref: OUT2020-0045

Dear Ms Scarafia,

I refer to your letter dated 7 May 2020.

The European Data Protection Board, as a principle, does not provide legal advice to individual data controllers. Therefore, we encourage you to enter into a dialogue with the competent national authorities.

In that regard, if the intended measures described in your letter are introduced by Amazon in several Member States, the EDPB encourages you to contact directly the lead supervisory authority and the other relevant national supervisory authorities as the measures can be subject to specific national provisions.

Yours sincerely,



Andrea Jelinek

Ms. Elizabeth Denham
UK Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire
SK9 5AF
United Kingdom

Ref: OUT2020-0110

Brussels, 20 October 2020

Dear Commissioner Denham,

Dear Liz!

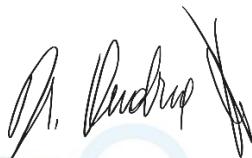
In response to your letter dated 14 September 2020, ICO/O/ED/L/RTL/0177, first I would like to thank you for ensuring that the ICO representatives participated in the EDPB Cooperation Expert Subgroup meeting on 22 September.

I also appreciate your readiness to discuss recent developments in EU data protection law, while I have at the same time to ensure that such dialogue is carried out by the EDPB, as for any other EU institution, agency or body, in compliance with the provisions of the EU-UK Withdrawal Agreement. This applies to cooperation between now and the end of the transitional period regarding, *inter alia*, remaining transnational cases or other issues that have an impact on the application of EU data protection rules in the U.K

In that context, I would like to inform you that the Cooperation expert subgroup will continue to work on the issue of cooperation procedures and will develop a framework of legal and practical criteria that will serve the smooth handling of ongoing cases. Special attention will be devoted to those cases where the ICO has been the lead authority so far. Whenever necessary and in compliance with the requirements of the Withdrawal Agreement, the EDPB will invite you to continue this exchange to anticipate as good as we can the potential impact of the Brexit on ongoing one-stop-shop cases.

Finally, I have no doubt that all EDPB members are willing to establish a constructive and fruitful relation with the ICO after the end of the transition period to the benefit of the protection of personal data.

Yours sincerely,



Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

20 October 2020

Europäische Akademie für
Informationsfreiheit und Datenschutz
z.Hd.
Dr. Alexander Dix
Bismarckallee 46/48
D - 14193 Berlin

by e-mail only

Ref: OUT2020-0111

Dear Dr. Dix,

Thank you very much for your letter regarding the guidance by the European Commission (EC) on Art 17 Directive (EU) 2019/790 on copyright and related rights (Copyright Directive).

Article 17 of the Copyright Directive provides for a new copyright liability regime for major online content-sharing service providers. In practice this means that there is an important shift from removing infringing content ex post through “notice and take-down”, i.e. to assess content after it has published, to an assessment of specific content before it is put online, without requiring any specific technical solution.

As you highlighted, the issue of upload filters and the possible impact on digital rights and fundamental rights is very important. The EDPB considers that any processing of personal data for the purpose of upload filters must be proportionate and necessary. Therefore, as far it is possible, no personal data should be processed when Art 17 Copyright Directive is implemented.

While this article provides that the platforms shall prevent future uploads of copyright-protected works, it does not as such stipulate that attempts to upload these material should be attributed to a specific data subject.

In the situation when the technical solution to comply with the obligations imposed by Article 17 of the copyright directive should nevertheless require processing of personal data or of electronic communication data, the GDPR and/or the ePrivacy Directive need to be considered, as required by Article 17 itself.

Where the processing of personal data is necessary, such as for the redress mechanism, such data should only concern data necessary for this specific purpose, while applying all the other principles of the GDPR. Regarding your second point, that neither the EDPB nor the EDPS nor any national SA has been involved in the drafting of the EC guidelines on Art 17, we can confirm that so far we have not received an official request by the EC for an opinion on this topic.

However, we continuously are in contact with the EC, who has presented this matter to one of our expert subgroups. Following this presentation, we have raised questions and provided comments on

the current work and issues that could require specific attention and we have signalled our availability for further collaboration on this matter.

Yours sincerely,

Andrea Jelinek



Brussels, 19 November 2020

Ref: OUT2020-0122

Subject: Letter of 13 July 2020 from News Media Europe and others

To whom it may concern,

I refer to your letter dated July 13th 2020, in which you raise questions on the French *Conseil d'Etat* decision of June 19th 2020¹, regarding which the *Commission Nationale Informatique et Libertés* (“CNIL”) has provided full information to the European Data Protection Board (“EDPB”) members.

First of all, the EDPB would like to underline that in the opposite of what may have sometimes been reported in the press, the French Court did not take a position on whether “cookie walls” are lawful or not on the merits, but considered that the CNIL could not set out a general and absolute ban of cookie walls in a soft law instrument like its guidelines on Article 82 of the French data protection act².

Furthermore, as the EDPB has stated numerous times³, the revision of the current ePrivacy Directive is an important and necessary step that has to be concluded rapidly. It is indeed the hope of the EDPB that the future ePrivacy Regulation provides clear answers to stakeholders, data subjects and Data Protection Authorities.

Until then, the EDPB recalls that the 2002 ePrivacy Directive, amended in 2009, remains the applicable legal framework, and that the consent under the ePrivacy Directive needs to meet the standards set by the GDPR. Indeed, recital 17 of the ePrivacy Directive states that “*For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes*”. In addition, Article 94(2) of the GDPR clearly states that “*References to the repealed Directive shall be construed as references to this Regulation*”.

The EDPB also recalls that, in line with Article 70(1)(e) GDPR, one of its tasks is indeed to examine, on its own initiative, on request of one of its members or on request of the Commission, any question

¹ Available here <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/434684>

² Available here <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337>

³ See for example the Statement of the EDPB 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, available here https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf

covering the application of the GDPR and issue guidelines, recommendations and best practices in order to encourage consistent application of the Regulation. The EDPB notably fulfilled this task when issuing the latest update of the EDPB guidelines on consent (Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, adopted on 4 May 2020).

Kindly note that the EDPB continues to follow carefully the evolution of the negotiations on the future ePrivacy Regulation and would like to thank you for your continued interest in the work of the EDPB.

Yours sincerely,



Andrea Jelinek

Moritz Körner MEP
European Parliament
Rue Wiertz 60
B-1047 Brussels
Belgium

03 December 2020

Ref: OUT2020-0131

Dear Mr. Körner,

I would like to thank you for your letter of 23 January 2020 regarding the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data for the purposes of the Terrorist Finance Tracking Program, the so called TFTP agreement.

Both of your questions go to the heart of the matter and reflect concerns which the European Data Protection Board also continues to share. More specifically, you raised questions, in the framework of the program, as to whether individuals can have their personal data corrected or deleted as well as to the amount of personal data collected and retained by U.S. authorities. I would like to respond to both of your questions in turn.

The TFTP agreement provides, in its Article 16, for the right of the individual to seek correction or deletion of his/her personal data processed by the US Treasury Department when the data is inaccurate or the processing contravenes the agreement. Such request must therefore be «duly substantiated» by the data subject, which implies that the requester has to be sure that his/her personal data is actually processed by the US authorities, and in particular the data subject has to know what precise data is processed in order to be able to spot any inaccuracy and ask for its rectification.

Consequently, it is only possible to guarantee the exercise of the right to correction or deletion if the right of access to such data is ensured as well. However, the TFTP agreement provides for a mechanism according to which any person has the right (as a minimum) to receive confirmation as to whether her or his data protection rights have been upheld in compliance with the agreement. Such a procedure might however result in a situation where the data subject is not informed of whether her or his data is stored in the TFTP database or whether any breaches to the agreement had to be remedied in response to her or his request. This broad and unverified restriction to the exercise of the right of access – expressly and specifically recognised as a fundamental right in Article 8(2) of the EU Charter of the Fundamental Rights – clearly prejudices the exercise of the other data subject's rights¹.

¹ It remains to be clarified in the review of the EU-U.S. Umbrella Agreement whether that agreement substantially improves the effectiveness of the right of access for the data subject.

I understand that such a response may be dissatisfactory to the requesting citizen. While it is to be noted that this situation corresponds to the provisions of the agreement, ratified by both parties, and that such provisions are also foreseen in other international agreements. The EDPB considers these provisions to be insufficient. In its recent *Schrems II* ruling, the Court of Justice of the European Union stressed again – in the context of personal data transfer to third countries – the importance and necessity of ensuring data subjects' rights' enforceability against authorities in the courts, in order to provide for an effective judicial remedy.

In this regard, I would like to recall however that data subjects can exercise their right to have their personal data corrected or deleted by sending a request to their competent national supervisory authority, which will transmit the request to the Privacy Officer of the United States Treasury Department. The TFTP agreement also foresees a joint review process in which individual members of the EDPB take part as experts for the European Commission. The reviews may improve the process in general and provide for some accountability.

With regard to the statement of DG HOME calling the amount of data collected in the framework of the agreement "big data", reference can be made to the Joint Supervisory Body (JSB) of Europol and its statement in 2015. The JSB stated in its report on the Europol's implementation of the TFTP agreement²: "*In this respect, the JSB likes to restate its assessment that due to the nature of the TFTP, the situation in terms of mass data transfer remains unchanged. The JSB restates that, in view of the nature of the TFTP and the scope of the agreement there is a massive, regular, data transfer from the EU to the US. There is a clear tension between the idea of limiting the amount of data to be transmitted by tailoring and narrowing the requests and the nature of the TFTP.*"³ It seems that the situation was still similar in 2019, as indicated by the reference in the EDPS TFTP inspection report where it is stated findings that "*the inspected requests [from the Treasury] are voluminous*".⁴

As regards the retention of the provided data, it follows from the Agreement that non-extracted data may be retained for five years. Such retention of non-extracted financial information continues to be of great concern to the EDPB, as it is also very problematic in view of the jurisprudence of the Court of Justice of the European Union⁵.

² Report 15/28, Joint Supervisory Body of Europol, Council of the European Union document 12338/15, p. 5

³ The EDPB notes the recommendation from the COM, in the 5th Joint review report on the implementation of the TFTP agreement, to minimise the amount of data requested by the designated provider. More specifically, it is recommended that the US Treasury should assess the message types and geographic regions that are the most and least responsive to TFTP searches. (Report from the Commission of 22 July 2019, COM(2019) 342).

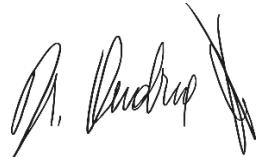
⁴ EDPS TFTP Inspection public report, of 28 May 2019, in

https://edps.europa.eu/sites/edp/files/publication/19-05-28_edps_inspection_report_art4_tftp_en.pdf

⁵ See in particular CJEU Opinion 1/15 of 26 July 2017 (EU-Canada PNR Agreement).

In view of these concerns, the EDPB would like to reiterate its call to review not only the PNR agreements, which face similar problems, but also the TFTP agreement with the United States.

Yours sincerely,



Andrea Jelinek

Recommendations



Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive

Adopted on 2 February 2021

Version history

Version 1.1	6 July 2021	Formatting change
Version 1.0	2 February 2021	Adoption of the Recommendations

Table of contents

1. INTRODUCTION	4
2. CONCEPT OF ADEQUACY	5
3. PROCEDURAL ASPECTS FOR ADEQUACY FINDINGS UNDER THE LED	6
4. EU STANDARDS FOR ADEQUACY IN THE POLICE COOPERATION AND JUDICIAL COOPERATION IN CRIMINAL MATTERS.....	8
A. General principles and safeguards.....	10
a) Concepts.....	10
b) Lawfulness and fairness of the processing of personal data	10
c) The purpose limitation principle	11
d) Specific conditions for further processing for other purposes	12
e) The data minimisation principle	12
f) The principle of data accuracy	12
g) The data retention principle	12
h) The security and confidentiality principle.....	12
i) The transparency principle (Article 13, Recitals 26, 39, 42, 43, 44, 46).....	13
j) The right of access, to rectification and erasure (Articles 14 and 16)	13
k) Restrictions on data subject rights.....	14
l) Restriction on onward transfers (Article 35, Recitals 64-65)	14
m) Accountability principle	14
B. Examples of additional principles to be applied to specific types of processing	15
a) Special categories of data	15
b) Automated decision making and profiling.....	15
c) Data protection by design and by default.....	15
C. Procedural and enforcement mechanisms	16
a) Competent independent supervisory authority	16
b) Effective implementation of data protection rules	16
c) The data protection system shall facilitate the exercise of data subject rights.....	16
d) The data protection system shall provide appropriate redress mechanisms	16

The European Data Protection Board

Having regard to Article 51 (1) (b) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA¹,

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

HAS ADOPTED THE FOLLOWING RECOMMENDATIONS

1. INTRODUCTION

1. The Working Party Article 29 (WP29) has published a working document² on adequacy referential under the General Data Protection Regulation (GDPR)³. This working document was endorsed by the European Data Protection Board (EDPB) at its first plenary.
2. As stated in Declaration N°21 annexed to the Lisbon Treaty, specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union (TFEU) may prove necessary because of the specific nature of these fields.
3. On this basis, the EU legislator adopted Directive (EU) 2016/680 (the Law Enforcement Directive, hereinafter the ‘LED’) laying down the specific rules with regard to the processing of personal data by competent authorities for the purposes of **the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against the prevention of threats to public security**.
4. The LED determines the grounds allowing the transfer of personal data to a third country or an international organisation in this context. One of the grounds for such transfer is the decision by the European Commission that the third country or international organisation in question ensures an adequate level of protection.
5. Where the working document WP254.rev01 on adequacy referential aims to provide guidance to the European Commission on the level of data protection in third countries and international organisations under the GDPR, the present document aims to provide similar guidance under the LED. It establishes in this context the core data protection principles that have to be present in a

¹ OJ L 119, 4.5.2016, p. 89.

² WP254.rev01 adopted by WP 29 on 28 November 2017 as last revised and adopted on 6 February 2018. It updates Chapter I of the Working Document ‘Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive’, WP12, adopted by WP29 on 24 July 1998.

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 26 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.

third country or an international organisation legal framework to ensure essential equivalence with the EU framework within the scope of the LED (i.e. for processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties). In addition, it may guide third countries and international organisations interested in obtaining adequacy.

6. The present document focuses solely on adequacy decisions. These are implementing acts of the European Commission according to Article 36(3) of the LED.

2. CONCEPT OF ADEQUACY

7. The LED sets the rules for the transfer of personal data to third countries and international organisations to the extent that such transfers fall within its scope. The rules on international transfers of personal data are laid down in Chapter V of the LED, in particular its Articles 35 to 39.
8. Pursuant to Article 36 of the LED, data transfers to a third country or an international organisation may take place if a third country, a territory or one or more specified sectors within a third country or an international organisation ensure an adequate level of protection. It stems from the Court of Justice of the European Union (CJEU) case law⁴ that this provision, must be read in the light of Article 35 of the LED, entitled ‘General principle for transfers of personal data’, which lays down that ‘all provisions [in Chapter V of the LED] shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined’.
9. Where the European Commission has decided that such adequacy level of protection is ensured, transfers of personal data to that third country, territory, sector or international organisation can take place, without the need to obtain any specific authorisation, except where another Member State from which the data were obtained has to give its authorisation to the transfer as provided in Articles 35 and 36 and Recital 66 of the LED. This is without prejudice to the need for the processing of data by the concerned Member States' authorities to comply with the national provisions adopted pursuant to Directive (EU) 2016/680.
10. This concept of ‘adequate level of protection’ which already existed under Directive 95/46⁵ and Council Framework Decision 2008/977/JHA⁶ has been further developed by the CJEU in this context and, recently, in the framework of the GDPR.
11. As specified by the CJEU, while the level of protection in the third country must be essentially equivalent to that guaranteed in the EU, ‘the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the European Union’ but ‘those means must nevertheless prove, in practice, effective’⁷. The

⁴ Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 16 July 2020, ECLI:EU:C:2020:559, §92 (Schrems II).

⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

⁶ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.

⁷ Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, ECLI:EU:C:2015:650, §§73 and 74 (Schrems I).

adequacy standard therefore does not require to mirror point by point the EU legislation, but to establish the essential - core requirements of that legislation.

12. In this context, the court also clarified that a Commission adequacy decision should contain any finding regarding the existence, in the third country, of rules adopted by this country intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to this third country, interference which the public entities of that country would be *authorised* to engage in when they pursue legitimate objectives, such as national security⁸.
13. The purpose of adequacy decisions by the European Commission is to formally confirm, with binding effects on Member States⁹ including their competent data protection authorities¹⁰, that the level of data protection in a third country or an international organisation is essentially equivalent to the level of data protection in the European Union. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors¹¹.
14. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules¹².

3. PROCEDURAL ASPECTS FOR ADEQUACY FINDINGS UNDER THE LED

15. In order to fulfil its task in advising the European Commission according to Article 51 (1) (g) of the LED, the EDPB should receive all relevant documentation, including relevant correspondence and the findings made by the European Commission. It is absolutely necessary, that all relevant documents are transmitted sufficiently in advance and translated into English to the EDPB to enable informed and useful discussions before the final adoption of adequacy decisions. Where the legal framework is complex, this should include any report prepared on the data protection level of the third country or international organisation. In any case, the information provided by the European Commission should be exhaustive and put the EDPB in a position to assess the analysis carried out by the Commission regarding the level of data protection in the third country or international organisation.

⁸ Schrems I, §88.

⁹ Article 288 TFEU.

¹⁰ Schrems I, §52.

¹¹ Recital 67 LED.

¹² Schrems I, §§72-74 and CJEU Opinion 1/15, on the draft agreement between Canada and the European Union, 26 July 2017, ECLI:EU:C:2017:592 (Opinion 1/15), § 134: ‘That right to the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law continues where personal data is transferred from the European Union to a non-member country. Even though the means intended to ensure such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from EU law are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union’.

16. The EDPB will provide an opinion on the European Commission's findings in due time, identifying insufficiencies in the adequacy framework, if any, and providing possible recommendations where necessary.
17. According to Article 36 (4) of the LED it is upon the European Commission to monitor - on an ongoing basis - developments that could affect the functioning of an adequacy decision.
18. Article 36 (3) of the LED provides that a periodic review must take place at least every four years. This is, however, a general time frame which must be adjusted to each third country or international organisation with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organisation in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.
19. Given its task to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organisation, no longer ensures an adequate level of protection, the EDPB must, in due time, receive meaningful information regarding the monitoring of the relevant developments in that third country or international organisation by the EU Commission. Hence, the EDPB should be kept informed of any review process and review mission in the third country or to the international organisation. The EDPB recommends being invited to participate in these review processes and missions, as it was foreseen in the Privacy Shield decision and is foreseen in the adequacy decision concerning Japan.
20. It should also be noted that, according to Article 36 (5) of the LED, the European Commission has the power, where the third country or international organisation no longer ensures an adequate level of protection, to repeal, amend or suspend existing adequacy decisions. The procedure to repeal, amend or suspend involves the EDPB by requesting its opinion in accordance with Article 51 (1) (g) of the LED.
21. Furthermore, without prejudice to the powers of prosecutorial authorities, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities or to engage in legal proceedings¹³. It stems in particular from the CJEU Schrems I ruling, that data protection authorities must be able to engage in legal proceedings before the national courts if they find a claim by a person against an adequacy decision well founded¹⁴. The Schrems II ruling confirmed this assessment¹⁵.

¹³ See Article 47 (5) LED and Recital 82 thereof.

¹⁴ See Schrems I, §65: 'It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity'.

¹⁵ See Schrems II, §120: 'Even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of his or her rights and freedoms in regard to the processing of personal data relating to him or her, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity'.

4. EU STANDARDS FOR ADEQUACY IN THE POLICE COOPERATION AND JUDICIAL COOPERATION IN CRIMINAL MATTERS

22. On substance, adequacy decisions should focus on the assessment of the existing legislation of the third country concerned as a whole, in theory and practice, in light of the assessment criteria set out in Article 36 of the LED. A third country or international organisation's system must contain the following basic general, procedural and enforcement data protection principles and mechanisms.
23. Article 36 (2) of the LED establishes the elements that the European Commission shall take into account when assessing the adequacy of the level of protection in a third country or international organisation.
24. In particular, the Commission shall take into consideration the rule of law, respect for human rights and fundamental freedoms¹⁶, relevant legislation, as well as the implementation of such legislation, effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are transferred, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organisation has entered into.
25. It is therefore clear that any meaningful analysis of adequate protection must comprise two basic elements: the content of the rules applicable and the means for ensuring their effective implementation in practice. It is upon the European Commission to verify – on a regular basis – that the rules in place are effective in practice.
26. The core of data protection general principles and procedural and enforcement requirements, which could be seen as a minimum requirement for protection to be adequate, are derived from the Charter of Fundamental Rights of the EU (Charter) and the LED. General provisions regarding data protection and privacy in the third country are not sufficient. On the contrary, specific provisions addressing concretely the right to data protection in the law enforcement area must be included in the third country's or international organisation's legal framework. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union. These provisions have to be enforceable.
27. Furthermore, regarding the principle of proportionality¹⁷, the CJEU held, in relation to Member State laws, that the question as to whether a limitation on the rights to privacy and to data protection may be justified must be assessed, on the one hand, by measuring the **seriousness of the interference** entailed by such a limitation¹⁸ and by verifying that the **importance of the public**

¹⁶ When assessing the legal framework of the third country, the possibility that death penalty or any form of cruel and inhuman treatment could be imposed on the basis of data transferred from the EU should be taken into account. Indeed, should such penalty or treatment be foreseen in the law of the third country, additional safeguards should be found in the third country legal framework to ensure that data transferred from the EU would not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment (e.g. an international agreement imposing conditions on the transfer, a commitment by the third country not to impose death penalty or any form of cruel and inhuman treatment on the basis of data transferred from the EU or a death penalty moratorium).

¹⁷ Article 52(1) of the Charter.

¹⁸ The court noted for instance that ‘the interference constituted by the real-time collection of data that allows terminal equipment to be located appears particularly serious, since that data provides the competent national

interest objective pursued by that limitation is proportionate to that seriousness, on the other hand¹⁹.

28. According to the case-law of the CJEU, a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned²⁰. Derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary²¹. In order to satisfy this requirement, besides laying down clear and precise rules governing the scope and application of the measure in question, the concerned legislation must impose minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. ‘It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing’²².
29. The EDPB has adopted Recommendations identifying essential guarantees reflecting the jurisprudence of the CJEU and the European Court of Human Rights (ECtHR) in the field of surveillance to be found in the law of the third country when assessing the interferences of such third country surveillance measures with the rights of data subjects in case the data are transferred to that third country under the GDPR²³. To assess whether Article 36(2)a) LED conditions are fulfilled, the EDPB considers that the guarantees set out in these Recommendations have to be taken into account when assessing the adequacy of a third country under the LED in the field of surveillance, bearing in mind further specific conditions in the field of surveillance in this context.
30. In relation to Article 36(2)b) requirement, the third country should not only ensure effective independent data protection supervision but also provide for cooperation mechanisms with the Member States' data protection authorities²⁴.
31. In relation to Article 36(2) c) requirement, apart from the international commitments the third country or international organisation has entered into, consideration should also be given to obligations arising from the third country's or international organisation's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations, in particular the third country's accession to other international agreements on data protection, e.g. the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account (Convention 108²⁵ and its modernised version, Convention 108+). The third country's compliance with principles enshrined in international documents such as the Council of Europe Practical Guide on the use of personal

authorities with a means of accurately and permanently tracking the movements of users of mobile telephones (...)’ (joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, 6 October 2020, ECLI:EU:C:2020:791, §187, including cited jurisprudence).

¹⁹ La Quadrature du Net and others, §131.

²⁰ Schrems II, §180.

²¹ Schrems II, §176, including cited jurisprudence.

²² Schrems II, §176, including cited jurisprudence.

²³ EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020.

²⁴ Recital 67 LED.

²⁵ Recital 68 LED.

data in the police sector: how to protect personal data while combatting crime may also be taken into account.

32. An adequacy decision should ensure that through the substance of privacy and data protection rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection, including for data in transit to this third country. As underlined by the CJEU in the Schrems II ruling, the high level of protection afforded should also be ensured while data are being transferred to a third country²⁶.
33. Finally, when adopting an adequacy decision with regard only to a territory or a specified sector in a third country, the European Commission should take into account clear and objective criteria, such as referring to specific processing activities or the scope of applicable legal standards and legislation in force in the third country²⁷.

A. General principles and safeguards

a) Concepts

34. Basic data protection concepts should exist. These do not have to mirror the LED terminology but should reflect and be consistent with the concepts enshrined in the European data protection law. By way of example, the LED includes the following important concepts: ‘personal data’, ‘processing of personal data’, ‘competent authorities’, ‘data controller’, ‘data processor’, ‘recipient’, ‘sensitive data’, ‘accuracy’, ‘profiling’, ‘data protection by design and by default’, ‘supervisory authority’ and ‘pseudonymisation’.

b) Lawfulness and fairness of the processing of personal data (Article 4 - Recital 26)

35. Under Article 8(2) of the Charter, personal data should, inter alia, be processed ‘for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’²⁸. However, in the context of law enforcement, it should be noted that the performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject should not provide a legal ground for processing personal data by competent authorities²⁹.
36. This legal basis should lay down clear and precise rules governing the scope and application of the relevant data processing activities and imposing minimum safeguards³⁰. In addition, the CJEU recalled that ‘legislation must be legally binding under domestic law’³¹.

²⁶ See §93.

²⁷ Recital 67 LED.

²⁸ See Schrems II, §173.

²⁹ Recital 35 LED also states that ‘[w]here the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties’.

³⁰ See Schrems II, §175 and §180 and Opinion 1/15, § 139 and the case law cited.

³¹ See case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, 6 October 2020, ECLI:EU:C:2020:790, §68 – It should also be clear that in the French version of the judgment, the CJEU uses the word ‘réglementation’ which is broader than only acts of Parliament.

37. To be lawful, the data processing³² should be necessary for the performance of a task carried out by a competent authority for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguards against and the prevention of threats to public security³³. These purposes should be provided in national law.
38. Personal data shall be processed fairly. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)³⁴.

c) The purpose limitation principle (Article 4)

39. The specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data³⁵.
40. Data should be processed for a specified, explicit and legitimate purpose within the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties³⁶, including the safeguarding against and the prevention of threats to public security within the third country and subsequently used for any of these purposes insofar as this is not incompatible with the original purpose of the processing, (e.g. for parallel enforcement proceedings or archiving in the public interest, scientific, statistical or historical use for such purposes) and subject to appropriate safeguards for the rights and freedoms of data subjects. If personal data are processed by the same or another controller (competent authority³⁷) for a purpose of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties other than that for which they have been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose³⁸. The existence of a mechanism to inform the relevant Member States' competent authorities of such further processing of data should also be taken into account³⁹. In addition, in any case the level of protection of natural persons provided for in the Union by the LED should not be undermined including in those cases where personal data are transmitted from the third country to controllers or processors in the same third country⁴⁰.

³² Processing of personal data wholly or partly by automated means, and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

³³ Competent authorities are any public authority competent for such purposes or any other body or entity entrusted by law to exercise public authority and public powers for such purposes.

³⁴ Recital 26 LED.

³⁵ Recital 26 LED.

³⁶ It includes ‘police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence’ (Recital 12 LED). It is to be distinguished from a national security purpose or from activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) (Recital 14 LED).

³⁷ See footnote 33.

³⁸ Recital 29 LED.

³⁹ Such mechanism could be for instance mutually agreed handling codes, a notification obligation under an international instrument, including possible automated notifications, or other similar transparency measures.

⁴⁰ Recital 64 LED.

d) Specific conditions for further processing for other purposes (Article 9)

41. Concerning further processing or disclosure of data transferred from the EU for other purposes than law enforcement purposes, such as national security purposes, it should also be provided by law, be necessary and proportionate. The existence of a mechanism to inform the relevant Member States' competent authorities of such further processing of data should also be taken into account⁴¹. Here as well, once further processed or disclosed, the data should benefit from the same level of protection as when they were processed initially by the receiving competent authority.

e) The data minimisation principle

42. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed. In particular, the application of data protection by design and by default requirements, such as limited entry fields (structured communications) or automated and non-automated quality checks, should be taken into account.

f) The principle of data accuracy

43. The data should be accurate and where necessary kept up to date. Nevertheless, the principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made⁴².
44. It should be ensured that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available⁴³ and that procedures are foreseen to correct or delete inaccurate data. In particular, any classification system of the information processed, as to the reliability of the source and as to the facts verification level⁴⁴, should be taken into account.

g) The data retention principle

45. Data should be kept for no longer than is necessary for the purposes for which they are processed. Appropriate mechanisms should be established for the erasure of personal data; it may be a fixed period or a periodic review of the need for the storage of personal data (or a combination of both: fixed maximum period and periodic review at certain intervals)⁴⁵. Personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use should be subject to appropriate safeguards (e.g. regarding access)⁴⁶.

h) The security and confidentiality principle (Article 29, Recitals 28 and 71)

46. Any entity processing personal data should ensure that the data are processed in a manner that ensures security of the personal data including by preventing unauthorised access to or use of personal data and the equipment used for the processing. This includes protection against, and

⁴¹ See footnote 39.

⁴² Recital 30 LED.

⁴³ Recital 32 LED.

⁴⁴ E.g. 4x4 grids for reliability assessments and handling codes.

⁴⁵ Article 5 LED.

⁴⁶ Recital 26 LED.

appropriate measures to address, unlawful processing as well as accidental loss, destruction or damage, using appropriate technical and organisational measures. When determining the level of the security, the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons should be taken into consideration.

47. Secure channels of communication between Member States' authorities transferring the personal data and third States' receiving authorities should be ensured.

i) The transparency principle (Article 13, Recitals 26, 39, 42, 43, 44, 46)

48. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing⁴⁷.
49. Information on all the main elements of the processing of their personal data should be made available to the individuals. This information should be easily accessible and easy to understand, using clear and plain language. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to them⁴⁸ and other information insofar as this is necessary to ensure fairness.
50. Some exceptions to this right of information may exist. Such limitation should however be allowed by a legislative measure and be necessary and proportionate to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others, as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned. Such restrictions should also be considered and assessed taking into account the possibility of lodging a complaint with a supervisory authority or seeking a legal remedy. In any case, any possible restriction should be temporary and not blanket and should be framed by similar conditions, safeguards and limitations to those required under the Charter and the ECHR, as interpreted in the case-law of the CJEU and by the ECtHR respectively, and in particular respect the essence of those rights and freedoms.

j) The right of access, to rectification and erasure (Articles 14 and 16)

51. The data subject should have the right to obtain confirmation about whether or not data processing concerning him/her is taking place and where that is the case, have access to his/her data. This right should at least comprise certain information about the processing such as the purposes of and legal basis for the processing, the right to lodge a complaint with the supervisory authority or the categories of personal data concerned⁴⁹. This is particularly important in case transparency is achieved through general notice (e.g. information on the authority's website).
52. The data subject should have the right to obtain rectification of his/her data for specified reasons, for example, where they are shown to be inaccurate or incomplete. The data subject should also have the right to have his/her data erased when for example their processing is no longer necessary or is unlawful.

⁴⁷ Recital 26 LED.

⁴⁸ Both the substantive rights (right of access, to rectification etc...) and the right to redress.

⁴⁹ Article 14 LED.

53. The exercise of those rights should not be excessively cumbersome for the data subject.

k) Restrictions on data subject rights

54. Possible restrictions to these rights could exist in order to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others, as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned. Such restrictions should also be considered and assessed taking into account the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

l) Restriction on onward transfers (Article 35, Recitals 64-65)

55. The onward transfers of personal data by the initial recipient to another third country or international organisation must not undermine the level of protection, provided for in the Union, of natural persons whose data is transferred. Therefore, such onward data transfers should be permitted only where the continuity of the level of protection afforded under EU law is ensured⁵⁰. In particular, the further recipient (i.e. the recipient of the onward transfer) should be a competent authority for law enforcement purposes⁵¹ and such onward transfers of data may only take place for limited and specified purposes and as long as there is a legal ground for that processing.

56. The existence of a mechanism for the relevant Member State's competent authorities to be informed and authorise such onward transfer of data has to also be taken into account. The initial recipient of the data transferred from the EU should be liable and be able to prove that the relevant competent authority of the Member State has authorised the onward transfer⁵² and that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision concerning the third country to which the data would be onward transferred⁵³.

m) Accountability principle (Article 4(4))

57. The controller should be responsible for and be able to demonstrate compliance with the data protection principles found in Article 4 of the LED.

⁵⁰ See also Opinion 1/15.

⁵¹ See footnote 33.

⁵² In this context, the existence of an obligation or a commitment to implement relevant handling codes defined by the transferring Member States' authorities should be taken into account.

⁵³ The above requirements are without prejudice to the specific conditions for onward transfers to an adequate country set out under the LED ((Article 35 (1) c and e)).

B. Examples of additional principles to be applied to specific types of processing

a) Special categories of data (Article 10 and Recital 37)

58. Specific safeguards should exist where ‘special categories of data’ are involved⁵⁴, addressing the specific risks involved⁵⁵. These categories should reflect those enshrined in Article 10 of the LED. Processing of special categories of data should therefore be subject to specific safeguards and only be allowed where strictly necessary under certain conditions for instance to protect the vital interest of an individual.

b) Automated decision making and profiling (Article 11 and Recital 38)

59. Decisions based solely on automated processing (automated individual decision-making), including profiling, which produce adverse legal effects or significantly affect the data subject, should only take place under certain conditions established in the third country legal framework⁵⁶.
60. In the European Union framework, such conditions include, for example, the provision of specific information to the data subject and the right to obtain human intervention on the part of the controller, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision.
61. The third country law should, in any case, provide for necessary safeguards for the data subject's rights and freedoms. In this regard, the existence of a mechanism to inform the relevant Member State's competent authorities of any further processing such as the use of the transferred data for large scale profiling, should also be taken into account.

c) Data protection by design and by default (Article 20)

62. When assessing adequacy, attention should be paid to the existence of an obligation for controllers to adopt internal policies and implement measures which adhere to the principles of data protection by design and data protection by default taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to adopt appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.

⁵⁴ Such special categories are also known as ‘sensitive data’ in Recital 37 LED.

⁵⁵ Such additional safeguards could be e.g. specific security measures, limited access rights for staff, restrictions as to further processing, automated decision-making, onward sharing or onward transfers.

⁵⁶ Opinion 1/15, § 173.

C. Procedural and enforcement mechanisms

63. Although the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union⁵⁷, a system consistent with the European one must be characterized by the existence of the following elements:

a) Competent independent supervisory authority (Articles 36(2)b and 36(3) and Recital 67)

64. One or more independent supervisory authorities, tasked with ensuring and enforcing compliance with data protection and privacy provisions in the third country should exist. The supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In that context, the supervisory authority should have all adequate enforcement powers to effectively ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able, on its own initiative, to conduct investigations. It should also be tasked with assisting and advising data subjects in exercising their rights (see also point c below). The adequacy decisions should identify, where applicable, that supervisory authority or authorities and the cooperation mechanisms with the supervisory authorities of the Member States to enforce data protection rules.

b) Effective implementation of data protection rules

65. A third country system should ensure a high degree of awareness among data controllers and those processing personal data on their behalf of their obligations, tasks and responsibilities, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as can systems of direct verification by authorities, auditors, or independent data protection officials.

66. A third country data protection framework should oblige data controllers or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority. Such measures should include keeping records or log files of data processing activities for an appropriate period of time. They may also include for example data protection impact assessments, the designation of a data protection officer or data protection by design and by default.

c) The data protection system shall facilitate the exercise of data subject rights (Articles 12, 17 and 46 LED)

67. A third country data protection framework should oblige data controllers to facilitate the exercise of data subject rights referred to under section A j) above and provide that its supervisory authority, upon request, inform any data subject concerning the exercise of their rights⁵⁸.

d) The data protection system shall provide appropriate redress mechanisms

68. Although there is currently no case law in relation to the adequacy of a third country legal system under the LED, the CJEU has interpreted the fundamental right to effective judicial protection as

⁵⁷ Schrems I, §74.

⁵⁸ The exercise of data subjects' rights could be either direct or indirect.

enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal⁵⁹ in compliance with the conditions laid down in that article.

69. According to settled case law of the CJEU, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter⁶⁰.
70. The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to ensure compliance.
71. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling any infringements of the right to data protection and respect for private life to be identified and punished in practice.
72. Where rules are not complied with, the data subject whose personal data are transferred to the third country should be provided as well with effective administrative and judicial redress in the third country, including for compensation for damages as a result of the unlawful processing of his/her personal data. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

⁵⁹ The CJEU considers that an effective judicial protection can be ensured not only by a court, but also by a body which offers guarantees essentially equivalent to those required by Article 47 of the Charter (see Schrems II, §197). This might be relevant in particular for international organisations.

⁶⁰ Schrems II, §§187 and 194, including cited jurisprudence.

Recommendations



Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions

Adopted on 19 May 2021

The European Data Protection Board

Having regard to Article 70(1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

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

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

HAS ADOPTED THE FOLLOWING RECOMMENDATIONS:

1. In the context of the COVID-19 pandemic the digital economy and e-commerce continuously developed. Analogously the risks of using credit card data online has increased. As stated by the Article 29 Working Party in its guidelines on Data Protection Impact Assessments, credit card data violations "*clearly involves serious impacts in the data subject's daily life*", as financial data can be used for "*payment fraud*"¹.
2. Therefore, it is very important that controllers put in place the appropriate safeguards for the data subjects, and to ensure them the control over their personal data, in order to decrease the risk of unlawful processing and foster trust in the digital environment. The EDPB deems this trust vital for sustainable growth of the digital economy.
3. For this purpose, these recommendations aim to encourage a harmonised application of data protection rules regarding the processing of credit card data within the European Economic Area (EEA), and to guarantee a homogeneous protection of data subject's rights, in full respect of the fundamental data protection principles as required by the GDPR.
4. More specifically, these recommendations deal with the storing of credit card data by online providers of goods and services, for the sole and specific purpose of facilitating further purchases by data subjects². They cover the situation where a data subject buys product or pays for a service via a website or an application, and provides his/her credit card data, generally on a dedicated form, in order to conclude this unique transaction.
5. As with any processing, the controller must have a valid legal basis under Art 6 GDPR to store those data. In this regard, it should be noted that a number of the legal bases mentioned in Article 6 GDPR would not be applicable to this situation and have to be excluded. The storage of credit card data following a transaction, in order to facilitate further purchases, cannot be considered necessary for compliance with a legal obligation (Art. 6(1)(c) GDPR) nor to protect the vital interest

¹ ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

² It should be noted that they do not cover payment institutions operating in online stores, nor public authorities. Neither the storage of credit card data for any other purpose, for instance for compliance with a legal obligation, or to establish a recurring payment in cases of contract of continuing performance or subscription for a long-term service (e.g. a contract which stipulates the supply of a certain good every month, or the subscription for a music or movie streaming service).

of a natural person (Art. 6(1)(d) GDPR). The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6(1)(e) GDPR) cannot be considered as an adequate legal basis either.

6. In addition, the storage of the credit card data after the payment for goods or services is not, as such, necessary for the performance of a contract (Art. 6(1)(b) GDPR). Whereas, in the first place, the processing of the data related to the credit card used by the client to pay is necessary to fulfil the contract, thereby triggering Article 6 (1)(b) GDPR, the storage of these data is only useful in order to facilitate the potential next transaction and facilitate the sales. Such purpose cannot be considered as strictly necessary for the performance of the contract for the provision of the good or service that the data subject has already paid³.
7. When it comes to a processing necessary for the purposes of the legitimate interest of the controller or a third party⁴, the EDPB notes that for the controller to be able to rely on Article 6(1)(f) GDPR, the three conditions laid down by this article must be satisfied⁵. This legal basis requires, first, the identification and qualification of a legitimate interest pursued by the controller or by a third party. The interest of the controller or third party may be broader than the purpose of the processing and must be present and effective at the date of the data processing⁶.
8. The legitimate interest legal basis requires, second, the need to process personal data for the purposes of the legitimate interest pursued. For what regards this last condition, provided that the controller has a legitimate interest as outlined above, it is not evident that the storage of the credit card data to facilitate future purchases is necessary to pursue that legitimate interest. Indeed, the actual conclusion of another purchase depends on the consumer choice and is not determined by the possibility to realize it “in one click”.
9. Finally, the third condition requires the performance of a balancing test: the legitimate interest of the controller or third party must be balanced against the interests or fundamental rights and freedoms of the data subject, including data subject rights to data protection and privacy. The balancing test requires taking into consideration the particular circumstances of the processing⁷. An essential component of the balancing exercise is the potential impact on the data subject’s rights and freedoms resulting from the processing⁸. Such impact can depend on the nature of data, specific method of processing and access to such data by third parties. Regarding the nature of

³ See as well EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subject, in particular on page 10.

⁴ See Article 29 Working Party Opinion on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, currently under revision by the EDPB (see the EDPB Work program 2021/2022 adopted on the 16 March 2021).

⁵ See CJEU judgement of 4 May 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA ‘Rīgas satiksme’, Case C-13/16, ECLI:EU:C:2017:336, point 28.

⁶ See CJEU judgement of 11 December 2019, TK v Asociația de Proprietari bloc M5A-ScaraA, Case C-708/18, ECLI:EU:C:2019:1064, point 44.

⁷ See CJEU judgement of 24 November 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, points 47 and 48; CJEU judgement of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779, point 62.

⁸ See CJEU judgement of 24 November 2011 abovementioned, point 44; CJEU judgement of 11 December 2019 abovementioned, point 56.

data criterion, it should be noted that financial data have been qualified by the Article 29 Working Party as data of a highly personal nature because their violation clearly involves serious impacts on the data subject's daily life⁹. Hence, notwithstanding the controller's obligation to implement technical and organisational measures to ensure appropriate security of the credit card data pursuant to Article 5(1)(f) GDPR and the fact that those data may be stored for other purposes, their processing to facilitate further purchases may involve an increasing risk of credit card data security breaches as it implies processing in other systems. Another important element of the balancing test that could be taken into consideration to assess the impact of the processing on data subjects' is the reasonable expectations of data subjects based on their relationship with the data controller, the context and the purpose of personal data collection¹⁰. Yet, it appears that at the time of purchase, while providing credit card data for the payment, the data subject does not reasonably expect his or her credit card data to be stored for longer than what is necessary to pay the goods or services he/she is buying. Consequently, the fundamental rights and freedoms of the person concerned by the data protection would likely take precedence over the controller's interest in this specific context.

10. Those aspects lead to conclude that consent (Art. 6(1)(a) GDPR) appears to be the sole appropriate legal basis for the above-described processing to be lawful. Indeed, to address the security risks, to allow the data subject to keep control over his/her data, and to decide actively of the use of his/her credit data, the specific consent of the data subject should be obtained before storing his or her credit card data after a purchase. This consent will enable the controller to demonstrate the individual's willingness to facilitate his/her further purchases through the specific website or application, which cannot be presumed by the simple fact he/she concluded one, or several, isolated transactions.
11. This consent cannot be presumed, it must be free, specific, informed and unambiguous¹¹. It must be delivered by a clear affirmative action, and should be requested in a user-friendly way, such as through a checkbox, which should not be pre-ticked¹², directly on the form used for the data collection. This specific consent must be distinguished from the consent given for terms of service or of sales and not be a condition to the completion of the transaction.
12. According to the Article 7(3) GDPR, the data subject shall have the right to withdraw his or her consent for the storing of credit card data for the purposes of facilitating further purchases at any time. The withdrawal must be free, simple and as easy for the data subject, as it was to give consent. It must lead to the effective deletion by the controller of credit card data stored for the sole purpose of facilitating further transactions.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁹ ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

¹⁰ See recital 47 GDPR.

¹¹ See EDPB Guidelines 05/2020 on consent under Regulation 2016/679.

¹² *Ibid.*

[Report]



1 December 2021

Report on responses received to the IMI Questionnaire



Table of Contents

1. Introduction	3
2. Summary of the responses received	3
2.1 General implementation of IMI in the member state	3
2.2 Data subjects' rights	4
2.3 Information policy in the member state	5
2.4 Implementation of IMI in the DPA	5
3. Conclusion and possible actions to be taken.....	6
ANNEX - Questionnaire	7



1. Introduction

In March 2021, a questionnaire was circulated to the members of the Coordinated Supervision Committee (CSC) regarding the use of the Internal Market System (IMI). The purpose of this questionnaire was to obtain information from the member states regarding the use of IMI in order to inform the further work of the CSC in this area.

Given that the purpose of the questionnaire was to obtain information on the use of IMI as a whole at the national level, and not only within the data protection authorities, CSC members coordinated the responses for part A of the questionnaire with their National IMI Coordinator.

The questionnaire consisted of four parts: questions about the general implementation of IMI in the member state (part A); questions about data subject rights (part B), questions about the information policy in the member state (part C) and questions about the implementation of IMI in the DPA (part D).

Twenty-eight responses were received from national DPAs, as well as responses from seven of the German Länder to part D of the questionnaire (within the response from the German Federal DPA).

The results of the questionnaire for each of the four parts are summarised in the following section, after which the report closes with some recommendations for possible actions to be taken by the CSC members.

2. Summary of the responses received

2.1 General implementation of IMI in the member state

National IMI Coordinators (NIMICs) are mostly located within ministries, mainly the ministry with responsibility for economics, commerce and/or trade. In some cases, the NIMIC is located within a governmental agency.

Delegated IMI Coordinators exist in a little more than half (17) of the member states that responded. One respondent clarified that delegated IMI coordinators exist only for certain modules. Another respondent clarified that the absence of delegated IMI Coordinators does not mean that there are no Coordinators apart from the NIMIC, as there is a Coordinator for each legal area (not a technical role) and that some IMI modules also require Coordinator roles. Another respondent stated that delegated IMI Coordinators only exist for the modules related to Directive 2005/36/EC on the recognition of professional qualifications and its respective implementing regulations. Another respondent stated that in addition to the NIMIC, there is a Coordinator at the level of the state, whose role is to support the competent authorities in their federal states (register authorities; provide user support and trainings etc.) The same respondent



explained that for some legal areas, there are also coordinators (not a technical role but more for legal and content matter), as well as for some IMI modules.

In terms of the tasks performed by NIMIC, according to the responses received, this is in line with what is foreseen in Art. 6 of the IMI Regulation¹, i.e. registering coordinators and competent authorities, acting as contact point, including with the European Commission, providing training etc. Other tasks mentioned include: IMI assistance and technical support, promotion of IMI use, monitoring the flow of information to the competent authorities and ensuring the smooth functioning of the system. One respondent pointed out that for some modules (e.g. GDPR) separate IMI coordinators are appointed to perform these tasks.

The number of national authorities using IMI ranges from 20 – 5517. Sometimes an approximate value was given, and two respondents pointed out that not all registered authorities are active users. One respondent explained that a significant number of the registered authorities are Trade Licensing Offices.

As regards the access allocation and procedure, generally this is the responsibility of the NIMIC in consultation with the responsible services for the specific modules. Two respondents mentioned that authorisations were given directly by the European Commission, in accordance with the procedure foreseen by DG GROW.

In terms of the authority roles in place, a wide range of responses was received. In some member states, the authority roles consist of competent authorities and coordinators, authority manager and access manager, or competent authorities and central authorities. In others, a number of different roles are foreseen, such as NIMIC, competent authorities, EPC authorities, EPC Coordinators, Alert Coordinators, Notification Coordinator, Notification Authorities and Alert Authorities. Some member states also foresee a role as observer.

The number of registered users of IMI ranges from 25 – more than 16, 000. In one case, this information was not available to the NIMIC.

Finally, as regards the general rules for assigning user rights, in most cases this is determined according to the rules of the competent authorities. Some respondents made reference to national legislation, while others referred to guidance provided by the European Commission, such as the IMI user handbook. Two respondents stated that there are no general rules in place.

2.2 Data subjects' rights

According to the majority of responses, data subjects' requests are handled directly by the competent authorities. Consequently, information on the number of requests was not available for most member states. Six respondents reported that there were no such requests, while three reported that either the NIMIC is not aware of such requests, or that there was no practical experience.

¹ Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation').



2.3 Information policy in the member state

The majority (22) of respondents reported that the NIMIC provides information about IMI on its website. Six respondents stated this is not the case.

The NIMIC informs about the rights of data subjects on its website according to a little more than half of the respondents. This includes providing a link to the IMI Regulation. One respondent stated that information is provided by the NIMIC on its website regarding the rights of data subjects, but not specifically related to IMI, as the NIMIC is not the data controller for IMI purposes. Of the thirteen respondents who stated that such information is not currently available, one respondent clarified that the NIMIC does not participate in exchanges, which involve processing of personal data, but that the NIMIC website includes a direct link to the Commission's IMI Website, where a dedicated data protection section is available. Another respondent stated that such information is not currently available, but will be provided in the future.

A little more than half of those who responded either consider that controllers do not provide sufficient information about IMI (10 respondents), or were not in a position to respond to this (6 respondents). Two respondents stated that the NIMIC reminds IMI actors of this regularly (for example during coordination meetings). One respondent stated that although it believes that the NIMIC provides sufficient information about IMI, it was unclear what is meant by sufficient information and where such quality requirements are specified. One respondent explained that it was not possible to answer this question as it would mean asking each authority directly. Similarly, another respondent, which replied that controllers do not provide sufficient information, stated that this was an assumption, because it was impossible to verify due to the high number of controllers.

2.4 Implementation of IMI in the DPA

As mentioned in the introduction, this part also includes the replies from seven of the German Länder DPAs. The total number of replies for this section is therefore thirty-five.

The number of users of IMI within the DPA range from 2- 95. One DPA made the distinction that only a small number (3 out of 17) have full access, while the remaining users have only viewer roles.

More than half of the DPAs which responded (18) do not have specific information about IMI on their website. In three cases, it was stated that this information was provided in the privacy notice, or in the annual report or that users are informed that complaints may be forwarded to the competent supervisory authority. In one case, it is planned to provide this information.

The majority (31) of DPAs which responded inform about the rights of data subjects on their website. Of these, it was clarified that in three cases this was not specifically related to IMI. Of the three DPAs which replied that this information is not currently provided on their website, one respondent stated that this was in preparation. One DPA did not respond to this question.



As regards the notification to data subjects once their information is entered in IMI, the replies showed that there are different approaches among the DPAs. In some cases, a written notification (e.g. by letter or email) is foreseen, while others do not foresee a specific notification. In some DPAs, general information is provided when the complaint is submitted, or on the DPA's website in the data protection and privacy statement or when it has been referred as a One Stop Shop (OSS) case. Three DPAs mentioned that the data subject's information is not systematically entered into IMI, but in cases where it is, a notification is provided.

More than half of the DPAs which responded (22) state that they maintain records of processing activities in relation to IMI. One DPA further clarified that this was part of the general documentation of "complaint handling" (including potential forwarding of the complaints). Another respondent clarified that this was only the case for those processing activities for which that DPA is the controller. For that DPA, the record for processing activities related to IMI are contained in a record named "Data Inspection Proceedings" which covers different information systems, including IMI. Of the 13 DPAs which replied that they do not currently maintain records of processing activities related to IMI, One DPA replied that this will be actioned for consideration by the DPA's DPO. Another respondent stated that their DPA is currently updating their records of processing activities and that the information provided in the DPA's website to the data subjects for the processing of their personal data includes the fact that in the process of examining a complaint the DPA may have to exchange personal data with other supervisory authorities (without mentioning explicitly IMI). This DPA does not consider IMI as a processing activity per se, but as an extension and part of the processing activities required to perform their duties as a supervisory authority.

3. Conclusion and actions to be taken

The responses to this questionnaire show some diversity among the member states in their use of IMI, in terms of the number of registered authorities and users, as well as the practice of access allocation, and the authority roles in place. In other areas, this was less the case, such as the tasks performed by the NIMIC, and the general rules for assigning user rights.

The responses further showed that in the majority of member states, data subjects' requests are dealt with directly by the controllers (i.e. the competent authorities) and there is therefore no centralised view in terms of the number of requests received.

In terms of the information policy at national level for IMI, a significant number of respondents (16 out of 28) indicated that they either considered that controllers do not provide sufficient information about IMI, or they were not in a position to respond to this. In order to address this issue and improve compliance, the CSC will prepare recommendations for the controllers regarding the obligation to communicate information to data subjects in accordance with Article 13 GDPR. These recommendations may be shared via the respective NIMIC and will also include a standard text, which may be used by controllers.



ANNEX - Questionnaire

Questionnaire on IMI

Purpose: To obtain information from the member states for the further work of the CSC

Member state: Please select your member state.

Query date: Please click here to enter a date.

A. Questions about the general implementation of IMI in the member state

1. Who is the National IMI Coordinator (NIMIC) in your member state?
Please click here to enter a text.

2. Are there Delegated IMI Coordinators (DIMICs) in your member state?
 yes no

3. What tasks does the NIMIC perform?
Please click here to enter a text.

4. How many national authorities use IMI?
Please click here to enter a text.

5. Who allocates access for authorities and what procedure is used?
Please click here to enter a text.

6. Which authority roles are in place within the member state?
Please click here to enter a text.

7. How many users are registered in the member state?
Please click here to enter a text.

8. Are there general rules for assigning user rights within the authorities?
Please click here to enter a text.

B. Questions about data subject rights

1. Who handles the data subject rights requests?
Please click here to enter a text.

2. How many inquiries per year does the responsible authority receive about data subjects' rights?



Access:

Please click here to enter a text.

Correction:

Please click here to enter a text.

Deletion:

Please click here to enter a text.

C. Questions about the information policy in the member state

1. Does the NIMIC provide information about IMI on its website?

yes no

2. Does the NIMIC inform about the rights of the data subject on its website?

yes no

3. Do all controllers of the member state provide sufficient information about IMI?

yes no

D. Questions about the implementation of IMI in the DPA

1. How many users of IMI does your DPA have?

Please click here to enter a text.

2. Does your DPA inform about IMI on its website?

yes no

3. Does your DPA inform about the rights of the data subject on the website?

yes no

4. Once the DPA enters the data subject's information into IMI, how will the data subject be notified?

Please click here to enter a text.

5. Do you maintain records of processing activities in relation to IMI?

yes no

Statement



Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)

Adopted on 2 February 2021

The European Data Protection Board has adopted the following statement:

Preliminary remarks and context of the EDPB statement

The European Data Protection Board (EDPB) and data protection authorities within the EU are following closely the development of the second additional protocol to the Budapest Convention and have regularly contributed to the consultation held by the Council of Europe, such as the annual « Octopus conference ». In November 2019, the EDPB also published its latest contribution to the consultation on a draft second additional protocol¹, indicating that it remained « *available for further contributions* » and called for « *an early and more proactive involvement of data protection authorities in the preparation of these specific provisions, in order to ensure an optimal understanding and consideration of data protection safeguards* »².

Following up on the publication of new draft provisions of the second additional protocol to the Budapest Convention³, the EDPB therefore, once again, wishes to provide an expert and constructive contribution with a view to ensure that data protection considerations are duly taken into account in the overall drafting process of the additional protocol, considering that the meetings dedicated to the preparation of the additional protocol are being held in closed sessions and that the direct involvement of data protection authorities in the drafting process has not been foreseen in the T-CY Terms of Reference⁴.

¹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf

² The EDPB upholds the positions and recommendations expressed in this previous contribution and considers relevant to restate key principles in light of the latest developments and new draft provisions published.

³ <https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations>

⁴ Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, Approved by the 17th Plenary of the T-CY on 8 June 2017, T-CY (2017)3.

The EDPB furthermore considers that the abovementioned provisions are likely to affect the substantive and procedural conditions for access to personal data in the EU, including as a result of requests from third country authorities, thus also resonating with ongoing debates at EU level and related legislative initiatives currently being considered by the co-legislators⁵. The EDPB therefore calls on the European Commission and European Parliament, as well as on EU Member States and national Parliaments, to ensure that the ongoing negotiations receive careful scrutiny in order to guarantee the full consistency of the envisaged second additional protocol with the EU acquis, in particular in the field of personal data protection.

Access to personal data across jurisdictions has already been addressed in the past by EU data protection authorities in various positions and opinions and the EDPB wishes to yet again recall in particular the Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in another jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime⁶, as well as its statement on data protection and privacy aspects of cross-border access to electronic evidence⁷. The European Data Protection Supervisor has issued Opinion 03/2019 on the mandate for the participation of the Commission in the negotiations⁸, as well as Opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters⁹. These contributions also build upon the EDPB Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters¹⁰.

The EDPB remains fully aware that situations where judicial and law enforcement authorities are faced with a "cross-border situation" with regards to access to personal data as part of their investigations can be a challenging reality and recognises the legitimate objective of enhancing international cooperation on cybercrime and access to information. In parallel, the EDPB reiterates that the protection of personal data and legal certainty must be guaranteed, thus contributing to the objective of 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 of the EU. The EDPB furthermore considers it essential to frame the preparation of the additional protocol within the framework of the Council of Europe core values and principles, and in particular human rights and the rule of law.

With regards to "trans-border direct access to stored computer data" as per Article 32(b) of the Budapest Convention, the EDPB reaffirms in particular that a data controller can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need

⁵ In particular, but not exclusively, the discussions on the Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters.

⁶ Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, 05/12/2013.

⁷ WP29 statement on data protection and privacy aspects of cross-border access to electronic evidence, 29 November 2017.

⁸ EDPS opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention.

⁹ EDPS opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters.

¹⁰ Opinion 23/2018 of the EDPB adopted on 26 September 2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters.

to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to its domestic law that will specify the purpose for which the data is required.

Since the Budapest Convention, as well as any of its additional protocols, are binding international instruments, the EDPB stresses that, in line with the CJEU case law, the “obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness”¹¹. It is therefore essential that EU negotiating parties ensure that the provisions laid down in the additional protocol do comply with the EU *acquis* in the field of data protection in order to ensure its compatibility with EU primary and secondary law.

Considering the timeframe of the consultation process, this EDPB contribution will focus on a preliminary assessment of the new draft provisions of the second additional protocol to the Budapest Convention which have not been subject to previous stakeholder consultations:

- Joint investigation teams and joint investigations
- Expedited disclosure of stored computer data in an emergency
- Request for domain name registration information

Once again, the EDPB understands that dedicated provisions on the protection of personal data are still being discussed. The EDPB remains available for further contributions and calls for an early and more proactive involvement of data protection authorities in the preparation of these specific provisions, in order to ensure an optimal understanding and consideration of data protection safeguards.

Provisional draft provisions on joint investigation teams and joint investigations (JITs) (Article 3), on the request for domain name registration information (Article 6) and on expedited disclosure of stored computer data in an emergency (Article 7)

On the basis of its preliminary assessment, the EDPB recommends further examining the provisional draft provisions with regard to the following elements.

The EDPB notes that both the requests for domain name registration information and for expedited disclosure of stored computer data in emergency cases are non-binding requests and grounds for refusal to comply with the request are not clearly defined, while the possibility to rely on the law of the requested State Party to refuse such cooperation, including grounds for refusal set out in MLATs, is also unclear¹². The EDPB recalls in this regard that the conditions under which the providers of electronic communications services or the entity providing domain name services must grant such access must be provided by law, so as to ensure that the processing relies on a clear legal basis.

¹¹ See CJEU joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461 - par (285).

¹² The draft Article 6 (2) refers to “reasonable conditions provided by domestic law” for instance.

The EDPB additionally refers to its previous contribution to reinstate that, except in cases of validly established urgency¹³ and, in light of the CJEU case law¹⁴, the EDPB considers that the type of requesting authorities who may issue such request should be limited to a prosecutor, a judicial authority or another independent authority. The EDPB also considers that the systematic involvement of judicial authorities in the requested parties is essential to ensure an effective compliance review of the requests with the Convention and to preserve the application of the principle of double criminality in the field of judicial cooperation.

The EDPB recalls in this regard that the double criminality principle aims at providing an additional safeguard to ensure that a Party cannot rely on the assistance of another to apply a criminal sanction, which does not exist in the law of this other Party. In addition to ensuring respect of individuals' rights and due process in the envisioned mechanism of judicial cooperation, such safeguard also provides for an essential guarantee related to the procedural conditions for access to their personal data. As already mentioned in its previous contribution, in relation to the security of data processing, the EDPB invites the T-CY to consider, as a specific data protection safeguard, a mechanism for the notification without delay of data breaches that could seriously interfere with the rights and freedoms of data subjects. Personal data breaches could indeed potentially have a range of significant adverse effects for individuals concerned.

In relation to the provisional draft provisions on the request for domain name registration information, the EDPB stresses that such information includes personal data and that therefore any international instrument laying down substantive and procedural conditions for accessing such data must, for the Parties members of the European Union, be compliant with EU primary and secondary law.

In relation to the provisional draft provisions on "expedited disclosure of stored computer data in an emergency" (Article 7), the EDPB notes that, depending on its application by each party, this new provision may involve the direct disclosure of content data. The EDPB also notes that the requested State Party may require, after the disclosure of the data, that a proper mutual assistance request is provided (Article 7(5)). In this latter case however, there is no commitment by the Parties to the envisaged Protocol, to delete the data or not to use it as evidence if, on the basis of the supplementary information obtained in the proper mutual assistance request, the requested authorities conclude that the conditions were not met to disclose the data. The legal consequences for the disclosed data, once in the requesting country, seem therefore to be completely left to the discretion of that country's national law. The lack of commitment at the level of the protocol therefore entails the risk to strip this provision of any protecting effect as to the processing of the personal data already disclosed.

The EDPB finally underlines the requirement under Article 52(1) of the Charter of fundamental rights of the EU¹⁵ according to which any limitations to the exercise of the rights and freedoms recognised by the Charter are subject to the principle of proportionality and may only be made if they are necessary. Therefore in order to be lawful under EU law, the draft provisions of the envisaged protocol

¹³ The EDPB notes that the notion of emergency is referred to within the meaning of paragraph 1 of the draft provision on Emergency Mutual Assistance and considers that the scope of such situation may be further clarified and framed.

¹⁴ See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (120)

¹⁵ See also Article 8(2) of the European Convention of Human Rights.

must fulfil this requirement. It then concerns both the personal data contained in the request as well as in the answer to such a request. **The EDPB is therefore particularly concerned by the wording of the draft Article 6(3) c and of the draft explanatory report, paragraph 13 in relation to this provision, which seem to imply that requesting third countries Parties to the envisaged Protocol may not be bound to comply with the principle of proportionality when addressing requests to an EU Member State.** In addition, there is not full clarity on the possibility under these provisions to invoke the proportionality principle as a ground for refusal.

It is also unclear whether Parties would be bound by the obligations to ensure, in the context of the envisaged protocol, the conditions and safeguards set out in Article 15 of the Budapest Convention¹⁶. **The EDPB recommends clarifying that the obligations set forth under Article 15 of the Budapest Convention fully apply also in the context of this cross-border cooperation.**

Provisions on data protection safeguards

The EDPB considers essential that the provisional text made public is complemented by dedicated provisions on data protection safeguards, which must then be assessed together with other provisions, in order to ensure that the draft additional protocol translates into a sustainable arrangement for the sharing of personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights.

The provisional draft provisions on request for domain name registration information and expedited disclosure of stored computer data in an emergency, by laying down procedural conditions for access to personal data, may already impact on the level of protection of personal data and may also need to be amended in order to ensure the operational application of appropriate data protection safeguards. **In this regard the EDPB would again like to point out the necessity that the data protection safeguards apply to any exchange of personal data in the context of the envisaged Protocol¹⁷, including in relation to the transfer of personal data¹⁸.**

The EDPB considers that specific provisions on data protection safeguards must reflect key principles and in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Likewise, the EDPB would like to stress the importance of ensuring core individual rights (access, rectification, erasure), with any restrictions limited by the principle of proportionality, and of effective judicial redress for data subjects for violations of the data protection safeguards. Exercise of these rights also requires notification of the data subject, at least once this no longer puts at risk the investigation. These principles, rights and obligations are also in line with the modernised Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), to which many Parties to the Budapest Convention on Cybercrime are also Party. In line with Convention 108+, they should apply to all authorities processing the data in the requesting Party, in order to ensure the continuity

¹⁶ See in particular Article 6(4) in brackets.

¹⁷ Article 6(4) seems to limit the application of the safeguards as well as of Article 15 of the Convention to the information disclosed only and not to the personal data included in the request.

¹⁸ According to the draft explanatory report, paragraph 9, the latter provision only may/should apply to the transfer of personal data pursuant to the joint investigations teams.

of protection. **The EDPB refers to its contribution in the public consultation in 2019 for further details on the EU requirements in this regard¹⁹.**

The EDPB reiterates the importance of involving data protection authorities in the drafting process of the additional protocol and stands ready to contribute and assist the T-CY in the preparation of provisional text of provisions on data protection safeguards.

For the European Data Protection Board

The Chair

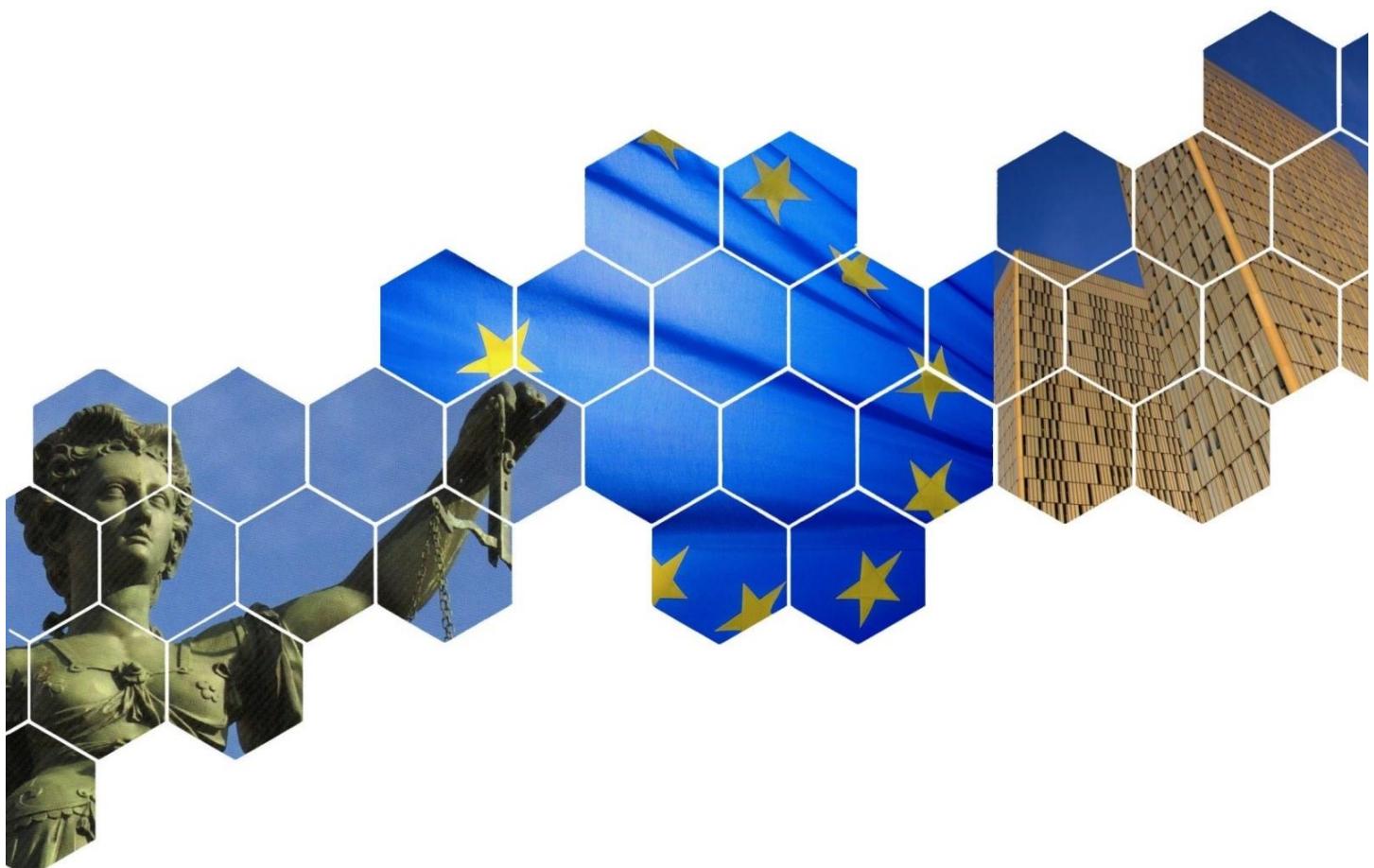
(Andrea Jelinek)

¹⁹https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf

Government access to data in third countries II

Final Report

Specific Contract No. 2022-0716
Implementing the Framework Contract EDPS/2019/02



This study has been prepared by Milieu under Contract No 2022-0716 (EDPS/2019/02) for the benefit of the EDPB.



The study has been carried out by researchers from CiTiP, KU Leuven, with the support of Milieu Consulting SRL. The authors of the study are Dr Laura Drechsler, Abdullah Elbi, Elora Fernandes, Eyup Kun, Isabela Maria Rosal, Bilgesu Sumer, and Dr Sofie Royer from CiTiP, KU Leuven.

The information and views set out in this study are those of the author(s) and do not reflect the official opinion of the EDPB. The EDPB does not guarantee the accuracy of the data included in this study. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for the use which may be made of the information contained therein.

This study does not bind the EDPB and its members in their assessment of individual data transfers. This study is not an “adequacy finding” for which the European Commission alone is competent under Regulation (EU) 2016/679 (GDPR) and Directive (EU) 2016/680 (LED).

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be; web address: www.milieu.be.

Table of contents

EXECUTIVE SUMMARY.....	4
1 INTRODUCTION	5
1.1 Objectives and scope of the study	5
1.2 Legal background	5
1.2.1 Data transfers in the GDPR	6
1.2.2 Interferences with the fundamental rights under the EU-Charter ...	6
1.2.3 Legality of governmental access	7
1.2.4 Objectives of general interest or protection of rights and freedoms of others	8
1.2.5 Necessity and proportionality	9
1.2.6 Respect the essence of the right.....	10
1.3 Study methodology	11
1.4 Structure of this report	11
2 IN DEPTH ANALYSIS OF BRAZIL	13
2.1 Rule of law, respect for human rights and fundamental freedoms	13
2.1.1 Context	13
2.1.2 Constitution.....	15
2.1.3 The Civil Rights Framework for the Internet in Brazil (MCI).....	15
2.1.4 The Brazilian General Data Protection Law	18
2.1.5 The Brazilian Data Protection Supervisory Authority (ANPD).....	20
2.1.6 Transparency rules in the public sector.....	22
2.1.7 Cybersecurity.....	23
2.1.8 Public security.....	24
2.2 Government access to personal data	25
2.2.1 Key considerations	25
2.2.2 National system of intelligence.....	26
2.2.3 Criminal prosecution.....	27
2.2.4 Data sharing	31
2.2.5 Oversight mechanisms.....	32
2.3 Data subject rights	34
2.3.1 Available rights and their scope of application	34
2.3.2 Redress mechanisms.....	35
2.4 Future legislation	36
2.5 Overview of relevant legislation	36
3 CONCLUSION.....	37
ANNEX 1 – QUESTIONNAIRE.....	38
ANNEX 2 – SOURCES OF INFORMATION.....	40
ANNEX 3 – ACRONYMS AND ABBREVIATIONS.....	49

EXECUTIVE SUMMARY

This report provides information on the legislation and practices in Brazil for the situation where personal data are accessed by governmental authorities for reasons of national security or law enforcement (governmental access). This study was based on a literature review via desk research (books, journal articles, databases and other online sources), also including reports of international organisations on the country in question. The legal analysis based on the literature review and the relevant legal documents was complemented by a round of interviews with carefully selected experts with the goal of gaining insights into the practice of the analysed laws. The main findings of this approach for each country are outlined in the following paragraphs.

In Brazil, the fundamental rights to privacy and to the protection of personal data are enshrined in the Constitution and can be exercised by all, including foreigners. The Brazilian General Data Protection Law (LGPD) represented a significant advance towards a more solid protection of personal data, being the result of years of multistakeholder discussions. The LGPD covers both public and private sector activities and has an extremely similar structure to the General Data Protection Regulation (GDPR). It also follows the *ex-ante* protection system and the accountability approach, sets a need for a legal basis for data processing, and establishes a minimum set of principles and data subjects' rights that must be observed in every processing of personal data. The Brazilian Data Protection Authority (ANPD), despite having started its activities only in 2020, already has a solid regulatory and personnel structure and is currently preparing for a more incisive action in concrete cases of rights' violation. Some activities of the State are, however, not in the scope of the LGPD, such as national security, public security, national defence, and criminal prosecution, which affects the level of protection provided in situations of governmental access. For such access, there are some laws and decrees in the Brazilian legal framework, as well as oversight mechanisms, which should enable *a priori* and *a posteriori* control of these activities. However, more comprehensive laws for data protection in these areas are still necessary for a full and solid protection of data subjects' rights in Brazil.

1 INTRODUCTION

1.1 OBJECTIVES AND SCOPE OF THE STUDY

According to Article 46 of the General Data Protection Regulation (GDPR)¹, data controllers and processors may transfer personal data to third countries or international organisations only if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Whereas it is the primary responsibility of data exporters and data importers to assess that the legislation of the country of destination enables the data importer to comply with any of the appropriate safeguards, supervisory authorities (SAs) play a key role when issuing further decisions on transfers to third countries. Hence, this report provides the European Data Protection Board (EDPB) and the SAs in the EEA/EU with information on the legislation and practice in Brazil on its government's access to personal data processed by economic operators. The report contains an overview of the relevant information in order for the SAs to assess whether and to what extent legislation and practices in Brazil imply massive and/or indiscriminate access to personal data processed by economic operators.

In order to answer the research questions, the study has

- investigated the general situation of Brazil with regard to the protection of fundamental rights and freedoms, by analysing international reports and findings from public bodies (e.g. Council of Europe, UN Human Rights Council and Human Rights Committee) and renowned non-governmental bodies (e.g. Amnesty International, Human Rights Watch, Privacy International). To this end, the study also identified the country's international commitments in the field of human rights, in particular of the right to privacy and data protection;
- analysed the legislation of Brazil in order to establish the substantive and procedural conditions for government access to personal data, including law enforcement and intelligence agencies. Specific attention was paid to the authorities involved in the adoption or amendment of the related rules, and entitled to authorise the governmental access to personal information;
- investigated whether specific purposes and conditions to access personal data of foreign individuals exist;
- identified, where existing, oversight mechanisms with regard to the governmental access to personal data, and to assess the independency from the executive of the bodies empowered to perform such control; and
- focused on rights and administrative or judicial redress mechanisms that are available to data subjects (including foreign individuals).

The study is not limited to an up-to-date overview of relevant legislation and case law, but also contains information with regard to the implementation of the legislation in practice, which has mostly been collected through interviews.

1.2 LEGAL BACKGROUND

This section gives an overview of the legal framework for assessing governmental access to personal data in a third country from the perspective of EU law, where such an assessment is required in the context of international personal data transfers under the GDPR². The main legal instruments considered are the EU-Charter of Fundamental Rights of the EU (EU-Charter), the European Convention of Human

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

² Article 46 GDPR.

Rights (ECHR) and the GDPR³.

1.2.1 DATA TRANSFERS IN THE GDPR

Personal data transfers to a third country or to an international organisation under the GDPR are only permitted if they comply with the requirements of Chapter V⁴. In principle, the GDPR allows the transfer of personal data to third countries or to international organisations based on three broad transfer tools, namely: (i) adequacy decisions; (ii) appropriate safeguards, i.e., legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, standard contractual clauses, codes of conduct, or certification mechanisms⁵; and (iii) derogations⁶. With these tools, the GDPR intends to provide a high level of protection to personal data transferred to third countries and international organisations⁷. Accordingly, the third country, international organisation or the transfer instrument, in case of appropriate safeguards, should provide guarantees, safeguarding a level of protection essentially equivalent to that ensured within the Union⁸. The Court has gradually developed the criteria for essential equivalence in *Schrems I*, *Opinion 1/15*, and *Schrems II*, which are relevant for all transfer mechanisms provided in the GDPR⁹.

1.2.2 INTERFERENCES WITH THE FUNDAMENTAL RIGHTS UNDER THE EU-CHARTER

Governmental access to personal data transferred from the EU to a third country or international organisation has been found by the CJEU to constitute an interference with Articles 7 (right to privacy), 8 (right to data protection), 21 (non-discrimination) and 47 EU-Charter (right to an effective remedy and fair trial). First, if communication data (content and/or meta-data) are maintained, accessed, and/or exposed by public authorities at the transfer's destination, this can constitute an interference with the fundamental right to privacy in Article 7¹¹. Second, there can be an interference with Article 8, when the transfer of personal data constitutes processing of such data¹⁰. Third, due to “*the risk of data being processed contrary to Article 21 of the Charter*,” the CJEU decided in *Opinion 1/15* that the transfer of special categories of personal data would require a precise and particularly solid justification¹¹. Fourth, the lack of effective remedies in a third country or international organisation in a situation of

³ Article 52(3) of the EU Charter states “*in so far this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.*” Therefore, the sought assessment needs to take place following the interpretation of both the CJEU and the European Court of Human Rights (ECtHR).

⁴ Article 44 GDPR.

⁵ Articles 46 and 47 GDPR.

⁶ Article 49 GDPR.

⁷ Article 44 GDPR ‘to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined’.

⁸ Recital 104 GDPR.

⁹ Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650, paragraph 64; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 105 and 188. The *Schrems II* decision is the first to explicitly address the issue of the level of protection necessary for international data transfers under the different transfer mechanisms of the GDPR. In this case, the Court clarified the connections between the various mechanisms and ruled that they should be all afforded essentially equal levels of protection to those provided by the GDPR. See judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 92.

¹⁰ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 124; and its paragraph 126: “*Those operations also constitute an interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the EU Charter since they constitute the processing of personal data*”; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 170 and 171; and its paragraph 83: the “[...] the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data [...]”.

¹¹ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 165; judgment of the Court of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 181.

governmental access can interfere with the fundamental right to an effective remedy in Article 47¹². However, none of the mentioned fundamental rights are absolute rights, thus where necessary, they can be limited following strict conditions listed in Article 52(1) of the EU-Charter.

According to Article 52(1) of the EU-Charter, an interference with a fundamental right can be justified, if it is (i) provided by law and (ii) respects the essence of the right, meaning that the interference must not empty the right of its core elements and prevent the exercise of the right. Furthermore, the interference must (iii) genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; and finally, (iv) it must be necessary and proportionate¹³.

1.2.3 LEGALITY OF GOVERNMENTAL ACCESS

According to Article 52(1) of the EU-Charter, any interference to a fundamental right of the EU Charter must be **provided for by law**. The CJEU holds that “*the legal basis which permits the interference [...] must itself define the scope of the limitation on the exercise of the right concerned*”¹⁴. The national laws permitting the interference shall lay down clear and precise rules governing the scope and application of the limitation¹⁵. As dissected in its elements below, the quality of law requirement is the first step when assessing if the interference is compatible with the EU-Charter¹⁶.

First, the law authorising the interference, e.g., the governmental access, must be “*accessible to the persons concerned and foreseeable as to its effects*”¹⁷. Foreseeability refers to the formulation of the law with sufficient precision to enable persons to regulate their conduct¹⁸. The level of such precision depends on the particular subject-matter¹⁹. For example, in the particular context of secret measures of surveillance, such as interception of communications, foreseeability cannot mean that individuals should be able to foresee when the authorities are likely to intercept their communications so that they can adapt their conduct accordingly²⁰. However, when executed secretly, the power granted to such secret activities may risk arbitrariness²¹.

In *Schrems II*, when assessing the US surveillance programme, the CJEU stated that “[...] *the legislation*

¹² Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 227. Although in this case, the interference with the PNR agreement was not found to be in violation with Article 47. See further judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 186.

¹³ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 124; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 82, 170-171.

¹⁴ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 227. Although in this case, the interference with PNR agreement was not found to be in violation with Article 47. See further judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 186.

¹⁵ Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 180.

¹⁶ The meaning of the expression ‘provided for by law’ should be in line with the ECtHR case law, which is frequently cited by the CJEU: an interference shall be based on a provision of law that has certain qualities, also known as the “quality of the law” requirement (judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, EU:C:2016:970; Opinion of Advocate General Saugmandsgaard delivered on 19 July 2016, paragraph 40). The CJEU has referred to a body of ECtHR case law in *La Quadrature du Net*, paragraph 128 in this regard: “*a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected*” (ECtHR, 28 October 1998, *Osman v. United Kingdom*, no. 23452/94, paragraphs 115 and 116; ECtHR, 4 March 2004, *M.C. v. Bulgaria*, no. 39272/98, paragraph 151. See also: ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 276).

¹⁷ ECtHR, 4 December 2015, *Zakharov v. Russia*, no. 47143/06, paragraphs 228-230; ECtHR, 16 February 2000, *Amann v. Switzerland*, no. 27798/95, paragraph 50; also see EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*, pp. 6-7.

¹⁸ ECtHR, 16 February 2000 *Amann v. Switzerland*, no. 27798/95, , paragraph 56; ECtHR, 2 August 1984, *Malone v. the UK*, , no. 8691/79, paragraph 66.

¹⁹ ECtHR, 26 April 1979, *The Sunday Times v. the UK*, no. 6538/74, paragraph 49.

²⁰ ECtHR, 18 May 2010, *Kennedy v. the United Kingdom*, no. 26839/05; , ECtHR, 29 June 2006, *Weber and Saravia*, no. 54934/00, paragraphs 152, 93-95.

²¹ ECtHR, 2 August 1984, *Malone v. the United Kingdom*, no. 8691/79, , paragraph 67; ECtHR, 24 April 1990, *Huvig v. France*, no. 11105/84, paragraph 29.

*in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question [...].*²² The possibility that the surveillance programmes allow access to data (even to data in transit) without sufficiently clear and precise limits was considered a violation of the legality of the governmental access²³. Such a law needs to have explicit, detailed provisions on surveillance procedures, providing individuals with a sufficient indication regarding the situations in which public authorities may execute surveillance measures and the conditions thereof²⁴. As will be further explained below, the legality of the interference is closely related to whether the limitation is necessary and proportionate²⁵.

1.2.4 OBJECTIVES OF GENERAL INTEREST OR PROTECTION OF RIGHTS AND FREEDOMS OF OTHERS

Governmental access needs to be strictly necessary to comply with **an objective of general interest or to protect the rights and freedoms of others**²⁶. An objective of general interest cannot be sought without considering how it must be reconciled with the fundamental rights impacted by the legislation. This is done by appropriately balancing the general interest goal against the rights in question²⁷. Therefore, the objective of general interest and the necessity and proportionality of the limitation are closely associated; it is essential to define and clarify the objective of general interest aimed by the limitation in satisfactory detail, as the necessity and proportionality test will be carried out against this context²⁸.

In that regard, it is worth referring to the case law of the CJEU on data retention, which discusses both the retention of personal data by private operators in order to be accessed by governmental authorities, and the conditions of such access²⁹. It is clear from the Court's case law that only the national security objective may justify public authorities having broad access to retained personal data in a general and indiscriminate manner (bulk access)³⁰. The national security objective must be linked to a genuine and present or foreseeable serious threat³¹.

²² “*It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted [...]*” judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 176.

²³ Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 180; see also judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650.

²⁴ ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 370.

²⁵ ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 334.

²⁶ Article 3 of the Treaty on the European Union, for instance, mentions freedom, security, and justice as general objectives. EDPB (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, p. 11. Article 23 of the GDPR states that data protection can legitimately be limited for security, defence, crime prevention, significant economic and financial interests, public health and social security, provided that the limitation respects the essence of the right to personal data protection and is necessary and proportionate. See also EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*. Relatedly, the CJEU in *Schwarz v. Stadt Bochum* found that processing personal data to prevent illegal entry to the EU pursued an objective of general interest (judgment of the Court (Fourth Chamber) of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670).

²⁷ Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, paragraph 52; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130.

²⁸ EDPS (2017), *Necessity toolkit*, p. 4.

²⁹ See *Privacy International*, paragraph 73: “*the mere retention of that data by the providers of electronic communications services entails a risk of abuse and unlawful access.*”

³⁰ Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, paragraph 31; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 166.

³¹ Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, paragraph 58; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168.

Targeted access to and retention of traffic and location data are considered by the CJEU to be a serious interference, thus such targeted access must be based on objective evidence which makes it possible to target individuals whose traffic and location data are likely to reveal a direct or indirect link with serious criminal offences³². Objective evidence has to be non-discriminatory, e.g., a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending³³. Moreover, on the basis of objective and non-discriminatory criteria, geographical areas characterised by a high risk of preparation for, or commission of serious criminal offences can be targeted.

An interference with fundamental rights of the EU Charter can also be justified if it is necessary to protect the rights and freedoms of others. The right to personal data protection often ambivalently interplays with other rights, such as freedom of expression and the right to receive and impart information. In such cases, courts must carry out a balancing exercise to settle the tension between the two³⁴.

1.2.5 NECESSITY AND PROPORTIONALITY

Fundamental rights and freedoms of the EU can be interfered with only if this is strictly necessary³⁵. This translates into the requirements of necessity and proportionality³⁶. Proportionality requires a balance to be struck between the importance of the public interest pursued and the seriousness of the interference with fundamental rights³⁷. Pursuant to the CJEU, proportionality necessitates the presence of minimal safeguards, such as enforceable rights and effective judicial review, in order to guarantee that interferences are “limited to what is strictly necessary”, as stated in *Schrems II*³⁸. Apart from the cases directly related to international personal data transfers, the CJEU has developed criteria on how to handle the necessity and proportionality assessments in its case law on data retention mentioned above³⁹. This case law should be considered relevant also for international personal data transfers that result in governmental access because it explains the limits to such access from the perspective of the EU-Charter⁴⁰.

The proportionality assessment extends to the access to and the use of retained data, which should also be limited to what is strictly necessary for the investigation⁴¹. Authorisation must be asked prior to

³² Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111 and judgment of the Court (Grand Chamber) of , 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18, and C-520/18, EU:C:2020:791, paragraph 148.

³³ Judgment of the Court (Grand Chamber) of 5 April 2022, C-140/20, *G.D. v The Commissioner of the Garda Síochána and Others*, EU:C:2022:258, paragraph 78.

³⁴ For example, the GDPR Article 85 states that the Member States shall reconcile by law the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic, academic, artistic, and literary expression. Freedom of expression and information is ensured by Article 11 of the EU Charter, and limitations on this right must fulfil the criteria in Article 52 (1), provided above. To achieve a balance between two fundamental rights, the limitations of the right to data protection must apply only insofar as strictly necessary (judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727, paragraphs 56-62).

³⁵ Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 176 and Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 140-141.

³⁶ According to the EDPS, the necessity test requires “*a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal*” (EDPS (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*, p. 27, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf). For other views on necessity see: Gerards, J., ‘How to improve the necessity test of the European Court of Human Rights’, *International Journal of Constitutional Law*, Vol. 11, No 2, April 2013, pp. 466–490, available at: <https://doi.org/10.1093/icon/mot004>.

³⁷ Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 130-131.

³⁸ Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 184.

³⁹ Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 35.

⁴⁰ EDPB (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, p. 7.

⁴¹ Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, paragraph 38.

access to the data, except in the event of a justified urgency⁴². This review must be carried out either by a court or an independent administrative body whose decision is binding. Moreover, means for individuals to obtain effective judicial and administrative redress should be in place⁴³. Data subjects need an effective possibility to access the retained data, obtain rectification, or erase data⁴⁴.

The ECtHR has developed minimum safeguards that the national law authorising governmental access should contain in the cases *Weber & Saravia v. Germany*,⁴⁵ *Roman Zakharov v. Russia*, and *Big Brother Watch and the Others*⁴⁶. Such laws need to include clear provisions on:

- the nature of offences that may give rise to a limitation;
- the categories of people liable to have their communications intercepted;
- a limit on the duration of interception;
- the procedure to be followed for accessing, examining, using and storing, communicating and destroying the data obtained;
- the precautions to be taken when communicating the data to other parties and the circumstances in which intercepted data may or must be erased or destroyed; and
- the review of the authorisation procedures and arrangements supervising the implementation of the measures along with any notification mechanism and the remedies provided⁴⁷. This last safeguard may come into play when (i) the surveillance is first ordered, (ii) while it is being carried out, or (ii) after it has been terminated⁴⁸.

1.2.6 RESPECT THE ESSENCE OF THE RIGHT

In some instances, an interference can be so extensive and invasive it empties an EU fundamental right of its essence⁴⁹. In this regard, the CJEU considered the law allowing public authorities to access, on a general basis, the content of electronic communications as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the EU-Charter⁵⁰. However, in *Digital Rights Ireland*, where the legislation in question did not permit generalised access to content data, the CJEU held that the limitation was not so intrusive as to impact the essence of the right⁵¹. *Schrems I* noted that legislation that does not provide any possibility to pursue legal remedies, e.g., access to or to rectify personal data, would be incompatible with Article 47 of the EU-Charter, ensuring the fundamental right

⁴² Judgment of the CJEU (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 120; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 137-139; judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratoraat*, C-746/18, EU:C:2021:152, paragraphs 40,53-54,58; ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 355.

⁴³ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 218-227.

⁴⁴ *Ibid*. See further judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 190.

⁴⁵ ECtHR, 29 June 2006, *Weber and Saravia*, no. 54934/00, also mentioned in judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 175; judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International*, C-623/17, paragraph 65.

⁴⁶ ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 54.

⁴⁷ ECtHR, 4 December 2015, *Zakharov v. Russia*, no. 47143/06, paragraphs 228-230; ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 335.

⁴⁸ ECtHR, 25 May 2021, *Big Brother Watch*, paragraph 336.

⁴⁹ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 124, 138-141, 150; EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*, p. 6.

⁵⁰ Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14 EU:C:2015:650, paragraph 94.

⁵¹ Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39.

to effective judicial protection⁵².

The essence of a right is interpreted by legal scholars in two ways. The first approach reads the notion as an absolute limit which is not subject to balancing⁵³. Following the first view, where the essence of a fundamental right is violated, the interference is unlawful without a further need for testing its necessity and proportionality⁵⁴. The second view links the essence to proportionality test as explained above⁵⁵. In this view, essence forms one component in the proportionality test.

1.3 STUDY METHODOLOGY

For this study, a literature review via desk research (books, journal articles, databases and other online sources) was conducted as the primary step. The purpose of this review was to map the law in the books, consisting of the relevant legal instruments and relevant case law. In addition, reports of international organisations were compiled in this step. After conducting a legal analysis of the collected sources, the loopholes in the knowledge in this area of law were defined. Thereafter, focus was laid on the law in action. A customised questionnaire was composed, tackling the higher defined loopholes (see Annex 1). This country questionnaire was priorly presented to the EDPB, making it possible to distribute the questionnaire to carefully selected experts in Brazil. To have a broad perspective, the researchers of this study strived to find persons working in different legal fields (academia, non-profit sector, the Bar ...).

We have carried out the following numbers of interviews:

- four stakeholders were interviewed, including one representative of the public sector, one of academia, and two lawyers/academics. In general, the interviews did not lead to fundamental changes of the content of the already collected information, but added only precise information.

Finally, the interviews were carefully analysed and compared with the results of the desk research. Where needed, anomalies were indicated. Based on this, the end report of the in-depth analysis was drafted including the results of the interviews.

1.4 STRUCTURE OF THIS REPORT

Section 2 describes an in-depth analysis of the legislation and practice on government access to personal data in Brazil.

⁵² Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650, paragraphs 64 and 95. The same conclusion regarding Article 47 was reached in *Schrems II*, where the Court stated: “According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter” (judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 187).

⁵³ “From a methodological perspective, the case law of the CJEU reflects the fact that court will first examine whether the measure in question respects the essence of the fundamental rights at stake and will only carry out a proportionality assessment if the answer to that first question is in the affirmative”. Lenaerts, K., ‘Limits on Limitations: The Essence of Fundamental Rights in the EU’, *German Law Journal*, Vol. 20, pp. 787, 779-793, Cambridge University Press, 2019. See further Brkan, M., ‘The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU’s constitutional reasoning’, *German Law Journal*, Vol. 20, pp. 864-883, Cambridge University Press, 2019.

⁵⁴ European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018, p. 44.

⁵⁵ Tridimas, T., Gentile, G., ‘The essence of Rights: An Unreliable Boundary?’, *German Law Journal*, vol. 20, pp. 794–816 and itsp. 804: “In short, although the concept of essence as a legal threshold must be understood as an autonomous limit, in effect, it is impossible to determine it without engaging in a balancing process which is best carried out through a proportionality analysis.”

First subsection aims to answer the research question concerning the general situation in Brazil as regards human rights, and specifically the right to privacy and data protection. It provides an overview concerning the rule of law, respect for human rights and fundamental freedoms. The main constitutional provisions are analysed, as well as the concrete application of such provisions in the national case law. The subsection also illustrates whether and how the right to privacy exists in Brazilian legal systems. Afterwards, the general findings by international organisations on the country's human rights situation are also briefly shown.

Subsequently, the country report includes a subsection illustrating the purposes, conditions, and oversight mechanisms of the governmental access to personal data. This subsection aims to answer the research questions related to the specific legislative requirements for government access to personal data; where specific provisions on foreign individuals' personal data do not always exist in the national legal system, the report also tries to address the research questions around the applicability of the Brazilian legislation to foreigners.

A subsection is dedicated to the data subjects' rights, their conditions for applicability and the redress mechanisms available to enforce them. The subsection's goal is to answer the research questions around individual rights and existing redress mechanisms as regards the right to privacy.

Section 3 provides conclusions by answering the research questions.

The annexes included to this study entail the exact questionnaire (Annex 1), a list of all the used sources (Annex 2) and an overview of the used acronyms and abbreviations (Annex 3).

2 IN DEPTH ANALYSIS OF BRAZIL

This section aims to answer the research questions of the study. The structure of the subsections is consistent with a division into areas of interests touched upon by the research questions. The answers are integrated in the related subsections. This section studies the situation in Brazil from the perspective of the rule of law and respect for human rights and fundamental freedoms; government access to personal data; and data subject rights. Any potential upcoming changes in the legislation are also discussed. Finally, the section contains an intermediary conclusion and a grid visually presenting the research results.

2.1 RULE OF LAW, RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

2.1.1 CONTEXT

Brazil is a democratic, liberal state, governed by the rule of law. Its Constitution (1988) states that Brazil is a representative democracy and a constitutional republic with a presidential system. The country follows the civil law legal system, based on codified laws, and is established as a federal state, meaning that it has distinct levels of government (federal, state, and municipal). It is a founding member of the United Nations, and a co-sponsor of the UN Resolution n. 68/167 — on the right to privacy in the digital age⁵⁶. It also ratified the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

The Organisation for Economic Co-operation and Development's (OECD's) Council has recently opened discussions about the accession of Brazil to it⁵⁷. In 2021, Brazil was an observer to the CoE Convention 108 meetings⁵⁸ and in 2022, Brazil has acceded to the Convention on Cybercrime, which has entered into force on the first of March 2023⁵⁹. Regionally, Brazil has ratified the American Convention on Human Rights.

Before the adoption of the Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados Pessoais* – LGPD, in the Portuguese acronym)⁶⁰ in 2018 (*infra* section 2.1.4), data protection rules were scattered around many different legal frameworks. They were included, for instance, in the Civil Rights Framework for the Internet, also called the Internet Bill of Rights (*Marco Civil da Internet* – MCI, in the Portuguese acronym)⁶¹, the Consumer Protection Code (*Código de Defesa do Consumidor* – CDC,

⁵⁶ Human Rights Council, A/HRC/27/3, *The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights*, available at: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.ohchr.org%2Fsites%2Fdefault%2Ffiles%2FDocuments%2FIssues%2FDigitalAge%2FA-HRC-27-37_en.doc%23%3A~%3Atext%3DIn%2520its%2520resolution%252068%252F167%2Ccommunications%2520and%2520the%2520collection%2520of&wdOrigin=BROWSELINK.

⁵⁷ OECD, *OECD takes first step in accession discussions with Argentina, Brazil, Bulgaria, Croatia, Peru and Romania*, 25 January 2022, available at: <https://www.oecd.org/newsroom/oecd-takes-first-step-in-accession-discussions-with-argentina-brazil-bulgaria-croatia-peru-and-romania.htm>.

⁵⁸ Council of Europe, *Brazil and the Data protection Commission of Gabon to join the Committee of Convention 108 as observers*, 12 October 2018, available at: <https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers->.

⁵⁹ Council of Europe, *Brazil accedes to the Convention on Cybercrime and six States sign the new Protocol on e-evidence*, 30 November, 2022, available at: <https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence>.

⁶⁰ Lei nº 13.709, de 14 de Agosto de 2018, *Lei Geral de Proteção de Dados Pessoais (LGPD)*, available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

⁶¹ Lei nº 12.965, de 23 de Abril de 2014, *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

in the Portuguese acronym)⁶², the Access to Public Information Law (*Lei de Acesso à Informação – LAI*, in the Portuguese acronym)⁶³, the Civil Code⁶⁴, the Good Payer's Registry Law (*Lei do Cadastro Positivo*, afterwards amended by Complimentary Law N. 166/2019)⁶⁵ and Interception of Telephone Communication Law (*Lei de Interceptação Telefônica*)⁶⁶. The patchwork of legal frameworks has received numerous criticisms, either due to the fragility of the protection of the data subject, or due to the legal uncertainty that this has caused. Actors from different sectors defended for years the need for a general data protection law, which took place in 2018 with the publication of the LGPD⁶⁷. This first general law on data protection in Brazil involved different stakeholders during the legislative process, and considered international standards and good practices in the data protection field.

The development of the LGPD was substantially influenced by the Convention 108 of the Council of Europe (CoE), the Directive 95/46/EC and the GDPR. Among other similarities to the GDPR, it also follows the ex-ante protection system and the accountability approach, sets a need for a legal basis for data processing, and establishes a minimum set of principles and data subjects' rights that must be observed in every processing of personal data. This is a result of the heavy public engagement in the drafting of the law⁶⁸.

The LGPD provisions became applicable on different dates: (i) in 2018, the rules relating to the structure and functioning of the Brazilian Data Protection Supervisory Authority (*Autoridade Nacional de Proteção de Dados – ANPD*, in the Portuguese acronym)⁶⁹ (pending the *de facto* creation of authority through the appointment, by the President of the Republic, of its directors); (ii) in 2020, the rest of the law, except the provisions concerning sanctions; and (iii) in 2021, the sanctions provisions.

The processing of data for the purposes of criminal persecution, national defence, State security or public safety do not fall under the scope of the LGPD. The law determines that this should be addressed in a separate legislation. Still according to the LGPD, any new legislation concerning these exceptions must lay down proportionate and strictly necessary measures to meet the public interest, while considering due process, data protection principles and data subject rights in the LGPD⁷⁰.

The Brazilian Constitution⁷¹ also contains some important provisions for the protection of personal data. It provides for the right to privacy in its Article 5º, X; the right to the secrecy of correspondence in its Article 5º, XII; and the *habeas-data* in Article 5º LXXII, a constitutional remedy that guarantees individuals the right to know whether their data are being processed by a public entity and, if necessary, the subsequent rectification. In 2022, the Constitution was amended to recognise the right to the protection of personal data as a fundamental right in the Brazilian legal order (Article 5º, LXXIX).

⁶² Lei nº 8.078, de 11 de Setembro de 1990, Dispõe sobre a proteção do consumidor e dá outras providências, available at: https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm.

⁶³ Lei nº 12.527, de 18 de Novembro de 2011, Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm.

⁶⁴ Lei nº 10.406, de 10 de Janeiro de 2002, Institui o Código Civil, available at: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm

⁶⁵ Lei nº 12.414, de 9 de Junho de 2011, Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm.

⁶⁶ Lei nº 9.296, de 24 de Julho de 1996, Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, available at: http://www.planalto.gov.br/ccivil_03/leis/19296.htm.

⁶⁷ Mendes, L. S., 'A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis', Caderno Especial LGPD, São Paulo, RT, November 2019, pp. 35-56.

⁶⁸ Ministério da Justiça e Segurança Pública, Governo lança debate público sobre regulamentação de lei e anteprojeto, 28 January 2015, available at: <https://www.gov.br/mj/pt-br/assuntos/noticias/governo-lanca-debate-publico-sobre-regulamentacao-de-lei-e-anteprojeto>.

⁶⁹ Autoridade Nacional de Proteção de Dados - ANPD, <https://www.gov.br/anpd/pt-br>.

⁷⁰ Article 4º, paragraph 1, LGPD.

⁷¹ Constituição da República Federativa do Brasil de 1988, available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

2.1.2 CONSTITUTION

The Brazilian Constitution foresees that “all persons are equal before the law, without any distinction whatsoever”. Therefore, all fundamental rights which include the rights to privacy and to the protection of personal data, are guaranteed to both Brazilians and foreigners residing in the country. Since 2020, data protection is openly considered a fundamental right in Brazil, due to a ruling of the Brazilian Supreme Federal Court (*Supremo Tribunal Federal* - STF, in the Portuguese acronym)⁷². As already mentioned, this right was enshrined in the Constitution itself in 2022. The new constitutional provision also determines that it is an exclusive federal competence to organise, oversee and draft bills on the right to the protection of personal data and data processing.

A relevant consequence of the ascension of data protection to the status of an autonomous fundamental right is that any proposal to abolish the right to data protection could not even be analysed by the National Congress (Article 60 paragraph 4º Constitution). This status also highlights the dual dimension of the fundamental right to data protection: (i) the subjective dimension, which concerns the individual protection against the risks of data processing while preserving the rule of law; and (ii) the objective dimension, which concerns the legislative duty of protecting personal data⁷³.

Even though the Constitution only mentions the protection of foreigners residing in the country, the Migration Law (*Lei de Migração*)⁷⁴ states that every person on national territory, residing in it or not, is entitled to the protection of fundamental rights, including the right to access to information and the guarantee of confidentiality of their personal data (Article 4º XIII Migration Law). Even though most judicial decisions regarding fundamental rights of foreigners only focus on the ones with permanent residency in the country⁷⁵, they are guaranteed to all individuals.

Regarding the activities carried out by public authorities, the Brazilian Constitution states they must follow the principles of legality, impersonality, morality, publicity, and efficiency (Article 37, Constitution). It is constitutionally established that public authorities and private legal entities are liable for damages that any of their agents, acting as such, cause to third parties (Article 37 paragraph 6º, Constitution), which may include the misuse of personal data⁷⁶.

2.1.3 THE CIVIL RIGHTS FRAMEWORK FOR THE INTERNET IN BRAZIL (MCI)

The MCI is the result of a bill proposed by civil society, which was drafted through an open and collaborative effort. Although the initial drafting of the bill and online public consultations started in 2008, it was only after Snowden’s revelations that the topic gained momentum in the Brazilian Congress and the bill entered into force in 2014.

⁷² Supremo Tribunal Federal, ADI 6387, 2020, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>.

⁷³ Supremo Tribunal Federal, ADPF 695/DF, 2022, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693>.

⁷⁴ Lei nº 13.445, de 24 de Maio de 2017, Institui a *Lei de Migração*, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o,&text=Art.,pol%C3%A3ticas%20p%C3%A3Blicas%20para%20o%20emigrante.

⁷⁵ For example, RE 587970/SP ruled that the social assistance foreseen in the Article 203, V, Constitution benefits Brazilians by birth, naturalised Brazilians and foreigners with residency in the country (Supremo Tribunal Federal, RE 587970/SP, 2017, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=2621386>); or RE 1018911/RR that states that the foreigner that demonstrates their lack of financial condition do not have to pay the fees to regularize their migration situation (Supremo Tribunal Federal, RE 1018911/RR, 2021, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5115280>).

⁷⁶ Autoridade Nacional de Proteção de Dados, *Tratamento de Dados Pessoais pelo Poder Público*, 2022, available at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>.

The main idea of the MCI was to translate the Brazilian Constitution into the online environment⁷⁷ and it is known to be based on three main pillars: freedom of expression, net neutrality and privacy. It establishes the principles, rights, obligations, and guarantees on the internet use in Brazil. Although data protection is not the direct focus of the MCI, it is one of its principles (Article 3º, III, MCI).

A series of rights is provided for by the MCI (Article 7º, MCI), which includes the right: (i) to the inviolability of intimacy and private life; (ii) to the inviolability and secrecy of the communication flow over the internet, unless otherwise ruled by a judicial decision; (iii) to the inviolability of stored private communication, unless otherwise ruled by a judicial decision; (iv) to obtaining information about the protection of connection and registries of access to internet apps; (v) not to have one's personal data shared with third parties; (vi) to obtain information about the processing of personal data, including its purposes; and (vii) to data erasure⁷⁸.

The rights to privacy, to the protection of personal data and the inviolability and secrecy of communication must be respected when at least a part of the processing of the personal data occurs on the national territory. This includes the situations in which a company located outside Brazil offers its services to the Brazilian population or has at least one establishment in the country (Article 10, MIC). The MCI also stipulates that contractual clauses that violate the rights to privacy, freedom of expression, as well as the inviolability and secrecy of private communications are to be considered invalid (Article 8º MCI).

The MCI also sets the need to consent for data processing (Article 7, VII, MCI), which seems to have been tacitly overridden by the LGPD, although there is still no official ruling on the matter. In Brazil, the Law of Introduction to the Rules of Brazilian Law (*Lei de Introdução às Normas do Direito Brasileiro* – LINDB in the Portuguese acronym)⁷⁹, provides, in its Article 2º that a subsequent law revokes the previous one when it expressly declares it, when it is incompatible with it or when it fully regulates the object of the previous law. It is also possible to understand the LGPD as a *lex specialis* when it comes to data protection. Certainly, the MCI was not revoked as a whole, but it is possible to interpret the tacit revocation of some of its provisions, such as the one referring to consent. Sanctions and data breaches are also topics of possible antinomy⁸⁰. The ANPD has recently published a new Regulation of Dosimetry and Application of Administrative Sanctions⁸¹, and has focused on the provisions set by the LGPD. This can reaffirm the special character of the LGPD.

The internet service and application providers, as defined by MCI, are responsible⁸² for keeping a register of internet connection and access to applications⁸³. Article 10 MCI states that safeguarding and making available these logs, together with personal data and the content of personal communication

⁷⁷ Souza, C. A., Viola, M., Lemos, R., *Brazil's Internet Bill of Rights: A Closer Look*, Instituto de Tecnologia e Sociedade, 2018, available at: https://itsrio.org/wp-content/uploads/2018/02/v5_com-capas_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf.

⁷⁸ In the MCI, data erasure is defined in its Article 7º, X, as the permanent erasure of personal data provided by the user to a given internet application, at their request, at the end of the relationship between the parties, except for the cases of mandatory record keeping provided for in the MCI and in the LGPD.

⁷⁹ Decreto-Lei n. 4.657, de 4 de setembro de 1942, *Lei de Introdução às Normas do Direito Brasileiro*, 1942, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm.

⁸⁰ Parentoni, L., Lima, H., 'Proteção de Dados Pessoais no Brasil: Antinomias Internas e Aspectos Internacionais', *Direito & Internet: Sistema de Proteção de Dados Pessoais*, 2019, pp. 483-512.

⁸¹ Autoridade Nacional de Proteção de Dados, *Resolução CD/ANPD n. 4, de 24 de fevereiro de 2023, Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas*, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucao4CDANPD24.02.2023.pdf>.

⁸² As established by Article 13, MCI, the responsible entity for the independent system must retain the connection logs for at least one year. Nonetheless, public authorities may require, as a precautionary measure, to extend this period; after 60 days of the preventive measure, the authority must ask for a judicial authorisation to access the data. In any case, sharing the registries requires a previous judicial order.

⁸³ As established by Article 15, MCI, the provider of applications must retain connection logs for internet application for six months. A judicial order may establish that other companies must work to retain said logs if the information is related to a fact and time. Public authorities can also, by a provisional measure, require a longer period of retention. However, in any case, the sharing of registries depends on a judicial order.

must be done in a way to protect user's intimacy, privacy, honour and image. Article 10 paragraph 3 MCI affirms that this does not prevent access to a person's registration data such as qualification, affiliation and address. Internet service and application providers can be obliged to share access logs and other personal data to identify an individual upon a judicial order (Article 10, paragraph 1º, MCI), as discussed below.

Content of communications can also be made available pursuant to a court order (Article 10, paragraph 2º MCI). However, the MCI does not oblige internet or application service providers to keep the content of communications, as it does for the registration of internet connections and access to applications (Article 14 et seq., MCI). This led to some legal disputes, including decisions that established the suspension of applications such as [REDACTED] after court orders requiring the provider to make the content of encrypted communication accessible to law enforcement authorities⁸⁴.

Any interested party may apply for a court order so that logs or the content of communications be included as evidence in a civil or criminal procedure. The competent judicial authority is then responsible for guaranteeing the secrecy of information when necessary. This authority can be a judge or a member of a Court if it is still possible to produce evidence in the procedure⁸⁵. According to Article 22, MCI, the application for a judicial order must include (i) well-founded evidence of the occurrence of the offence; (ii) reasoned justification of the usefulness of the records requested for investigation or for evidence purposes; (iii) the period to which the records refer. In addition, the judge is called to take appropriate measures to protect, *i.a.*, private life. In light of this, an intrusion to private life would need to meet the criteria of (i) proportionality; (ii) necessity; (iii) responding to a public interest and (iv) providing appropriate measures to protect the right to privacy.

The MCI does not directly address the topic of data transfers to third countries. In relation to data processed within the scope of the MCI, the LGPD would normally apply to data transfers (where this is also within the scope of the LGPD). Article 11, MCI, also reinforces that the Brazilian legislation and, specifically, the rights to privacy, to the protection of personal data, and the secrecy of private communication and records must be observed whenever at least part of the logs, data processing or communication is carried out within the national territory. The same applies to situations when the processing activities are done by an international company, as long as it offers services to the Brazilian market or when at least one member of the same economic group has an establishment in Brazil.

Although this directly regulates the activities of companies in Brazil, in a recent decision⁸⁶, the STF deemed constitutional that Brazilian authorities request information directly from those entities that are covered by the scope of Article 11, MCI, without having to use, in the specific case, the MLAT agreement with the United States of America, as will be further developed below. As justified by the STF, this model is aligned with other countries' models such as Canada, Norway, Spain and Belgium⁸⁷.

In cases where Article 10 and 11, MCI, are not observed, without prejudice to other civil, criminal or administrative sanctions, internet connection or application providers may (i) receive a warning,

⁸⁴ It is important to note that the discussion on the constitutionality of suspending [REDACTED] applications for law enforcement based on the MCI has reached the STF, but court proceedings have been paralysed since 2020 (see Supremo Tribunal Federal, ADI 5527, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>, and Supremo Tribunal Federal, ADPF 403, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500>). So far, only two STF justices have published their votes. Both converged in the sense of ruling out the interpretation that considers possible the breaking (or weakening) encryption through a court order for accessing the content of messages with law enforcement purposes. Thus, they argue that it is not possible to impose the penalties of the MCI when they imply breaking encryption. (Vlois, R., 'Tecnoautoritarismo e o bloqueio de provedores por descumprimento de ordens judiciais no Brasil', *Nexo Jornal*, 26 January 2023, available at: <https://pp.nexojornal.com.br/opiniao/2023/Tecnoautoritarismo-e-o-blockio-de-provedores-por-descumprimento-de-ordens-judiciais-no-Brasil>).

⁸⁵ In criminal cases, there is a judge involved since the investigation phase. The investigating judge will work on guarantying the fundamental rights during the course of investigation.

⁸⁶ Supremo Tribunal Federal, ADC 51, 2023, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>.

⁸⁷ Supremo Tribunal Federal, ADC 51 – Constitucionalidade do Mecanismo Previsto no MLAT, available at: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/briefingGabineteADC51.pdf>.

indicating a deadline for adopting corrective measures; (ii) receive a fine of up to 10 % of the revenue of the economic group in Brazil; (iii) undergo temporary suspension of activities involving the acts provided for in Article 11; or (iv) be prohibited from carrying out activities involving the acts provided for in Article 11.

2.1.4 THE BRAZILIAN GENERAL DATA PROTECTION LAW

The LGPD applies to the public and private sector, if the processing of personal data takes place in the national territory⁸⁸; if its purposes are related to the offering of services or goods to the Brazilian population; or if the data has been collected in the national territory⁸⁹. These situations do not depend on the nationality of the data subject, meaning that foreigners will also have their rights guaranteed if their data are being processed under one of these circumstances.

As mentioned earlier, the LGPD does not apply in certain situations, such as when data is being processed for purposes of public security, national defence, State security, or investigation and repression of criminal offences (Article 4º III LGPD). These purposes listed will need to be regulated by specific law, according to the LGPD, which must provide for proportional and strictly necessary measures to serve the public interest, observing due process of law, the general principles of protection and the rights of the holder provided for in the LGPD (Article 4º, paragraph 1º LGPD). The law also establishes that private entities are prohibited to process data for these purposes, unless they work under the supervision of a public authority. In these cases, there is a specific obligation of informing the ANPD⁹⁰. Finally, the ANPD must issue technical opinions or recommendations regarding these exceptions and request data protection impact assessments from competent authorities (Article 4º, paragraph 3º LGPD).

According to the LGPD, the processing of personal data must respect certain principles⁹¹ and it can only take place if there is a legal basis. The relevant legal provisions can be different when it comes to special categories of data⁹². It is important to mention that it is still not clear which legal bases apply to the

⁸⁸ The LGPD defines processing as: any operation carried out with personal data, such as those referring to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, diffusion or extraction (Article 5º, X). Thus, as long as one of these steps happens in Brazilian territory, the processing must comply with the LGPD, including if the collection happened in another country and the data were then transferred to Brazil.

⁸⁹ The data collection is considered to take place in the national territory if the data subject was in Brazilian territory at the moment of the collection.

⁹⁰ Article 4, paragraph 2º, LGPD. The supervision of the public authority should be understood as the fact that the public body is responsible for the decisions of the processing, sub-contracting a private company as a processor. Also, Article 4, paragraph 4º, LGPD, establishes that in any case the full length of a database related to these purposes can be processed by a private entity, unless this company is completely composed of public capital.

⁹¹ Article 6º, LGPD states that data processing must respect the following principles: purpose limitation; suitability for the purpose of data processing; necessity and proportionality; free access to data by the data subject; data quality; transparency; security; prevention; non-discrimination; accountability.

⁹² The special categories of data include sensitive data and data of children and adolescents. Sensitive data is defined as any data about race or ethnic origin, religious beliefs, political opinion, union membership, affiliation to a religious, philosophical or political organisation. It is also considered as sensitive data regarding the health or the sexual life of an individual, or any genetic or biometric data (Article 5º, II LGPD). For processing general personal data, the legal bases that can be used are (Article 7º, LGPD): consent; legal or regulatory obligation; execution of public policies; conducting studies by research body; execution of contracts or preliminary procedures; regular exercise of rights in judicial, administrative or arbitration proceedings; protection of life or physical safety of the data subject or third party; health protection; legitimate interest; and credit protection. For processing sensitive data (Article 11, LGPD), the legal bases of legitimate interest, credit protection and execution of contracts or preliminary procedures are not allowed. However, the LGPD includes for these cases another legal basis: the prevention of fraud and security of the data subject, in the processes of identification and authentication of registration in electronic systems. For processing children's data, the LGPD is not clear if all the legal bases related to general and sensitive data apply (the ANPD is currently working on this issue after having opened a public consultation). However, Article 14, LGPD, provides specific rules on consent, stipulating that it may be given by persons aged 12 and over. It also provides specific legal bases in cases where the consent of children under 12 years old cannot be collected in its Article 14 paragraph 3º (to contact parents or the legal guardian, or for the child's protection).

public sector⁹³. In 2020, the STF ruled that execution of public policies was the only possible legal basis from Article 7º (general data) and 11 (sensitive data) that could be applied to data sharing by the public administration. Based on this interpretation, the court understood that specific provisions in Chapter IV, LGPD, would provide extra legal bases for the processing of personal data by the public sector. Article 23, LGPD, for example, would allow the processing of personal data for the execution of legal competences or attributions of public services.

In an apparent different direction, a guideline published by the ANPD on data processing by the public sector establishes that any of the legal bases defined in the LGPD, either in Article 7º or 11, can be used by the public sector. When it comes to consent and legitimate interest, the examples are related to activities that have no direct correlation with public functions⁹⁴. Beyond the legal basis of execution of public policies, the ANPD established that the fulfilment of a legal or a regulatory obligation is a relevant and applicable legal basis for data processing for public authorities.

The LGPD also establishes some data subject rights, including the right to access, rectification, portability, information, request for anonymisation, blocking or erasure of data processed in discordance with the law, and request the erasure of data processed by consent. These will be further discussed below (*infra*, section 2.4).

International data transfers are only allowed within the LGPD framework when (Article 33 LGPD):

- the third country or international organisation provides an adequate level of protection of personal data, aligned with the LGPD⁹⁵;
- there are adequate guarantees of compliance with the principles and data subject rights provided by the LGPD, in the form of
 - specific contractual clauses for a given transfer;
 - standard contractual clauses;
 - global corporate norms; or
 - regularly issued stamps, certificates or codes of conduct.
- the data transfer is necessary for international legal cooperation between public intelligence, investigative and criminal prosecutorial agencies, in accordance with the instruments of international law;
- the transfer is necessary to protect the life or physical safety of the data subject or a third party
- the ANPD has provided authorisation
- the transfer is related to an agreement undertaken through international cooperation
- the data subject has provided his/her specific and highlighted consent for the transfer, having received prior information on the international nature of the operation, clearly distinguishing it from other purposes;
- necessary for compliance with a legal or regulatory obligation by the controller;
- necessary for the performance of a contract or preliminary procedures related to a contract to which the data subject is a party, at the request of the data subject;
- necessary for the regular exercise of rights in judicial, administrative or arbitration proceedings.

⁹³ Wimmer, M., ‘O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público’, *Tratado de Proteção de Dados Pessoais*, 1. ed., Rio de Janeiro, Forense, 2021. pp. 271–288.

⁹⁴ The guideline explains that consent will not be the most appropriate legal basis for processing personal data by the Public Sector, notably when the processing is necessary for the fulfilment of legal obligations and attributions. In those cases, the body or entity exercises typical state prerogatives, which are imposed on the subject in a power imbalance relationship, in which the individual does not have effective conditions to freely express themselves (e.g., registering in a public university). Therefore, consent cannot be used, as a rule, for public activities purposes. The same applies for the legitimate interest, where the public authority must verify the proportionality of the processing (e.g., information security activities) (Autoridade Nacional de Proteção de Dados, *Tratamento de Dados Pessoais pelo Poder Público*, January 2022, available at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>.

⁹⁵ The ANPD has still not issued any adequacy decisions.

Although the structure of the LGPD, when it comes to data transfers, is quite similar to the GDPR, there are important differences. According to national experts, for example, there is no hierarchy between the different possibilities for international data transfers and any of the legal grounds are valid. So far, the ANPD has not issued adequacy decisions. It is also important to note that although public intelligence, investigative and criminal prosecution activities are not within the scope of the LGPD, Article 33 foresees these activities as a legal ground for data transfers.

When a controller or data processor violates the LGPD, they are subject to redress mechanisms (*infra* section 2.3.2) and also to administrative sanctions applied by the ANPD. The possible administrative sanctions are:

- a warning, with an indication of the deadline for adopting corrective measures;
- a fine of up to 2 % of the income of the private legal entity, group or conglomerate in Brazil in its last fiscal year, excluding taxes, limited in total to R\$ 50 000 000.00 (fifty million reais) for infringement;
- a daily fine, limited in total to R\$ 50 000 000.00 (fifty million reais) for infringement;
- the publication of the violation after its occurrence has been duly investigated and confirmed;
- the suspension of the processing of the data related to the violation until its regularisation;
- the erasure of the personal data related to the violation.

2.1.5 THE BRAZILIAN DATA PROTECTION SUPERVISORY AUTHORITY (ANPD)

The ANPD was first envisioned as an independent body in the LGPD. However, the creation of a new agency in Brazil by the legislative power was considered unconstitutional by the president of the republic at the time, which argued that only the executive branch was competent to do so. Despite having sanctioned the LGPD, the former president vetoed the provisions related to the ANPD and issued the Provisory Measure (MP) n. 869/2018⁹⁶, creating it as a body connected to the Presidency of the Republic – thus eliminating the financial and political autonomy of the authority. The ANPD started its activities only in November 2020, after the nomination of the first directors of the authority.

In 2022, another Provisory Measure⁹⁷ modified the LGPD and turned the ANPD into a ‘special nature autarchy’, which means that it is autonomous and independent for its decisions and normative publications. More recently, a Presidential Decree⁹⁸ linked the ANPD to the Brazilian Ministry of Justice and Public Safety, putting an end to its direct connection with the Presidency of the Republic. The affiliation with the Ministry of Justice and Public Safety was important since the Ministry is historically linked to the protection of fundamental rights. It also does not affect the independence of the ANPD, since this is now foreseen by law. This administrative change only guarantees that the Ministry, and not the Presidency, is the public body responsible for providing administrative support to the ANPD, such

⁹⁶ Transformed into Law n. 13.853/2019 (*Lei nº 13.853, de 9 de Julho de 2019, Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm).

⁹⁷ MP n. 1124/2022, transformed into the Law n. 14.460/2022 (*Lei nº 14.460, de 25 de Outubro de 2022, Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019*, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14460.htm).

⁹⁸ Decreto nº 11.348, de 1º de Janeiro de 2023, *Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão e funções de confiança*, available at: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm.

as personnel and infrastructure⁹⁹. It is important to mention that the speed of the ANPD independence procedure was due to the fact that it was also a national priority. Brazil plans ascending to the OECD and having an independent DPA was formally recommended to the Brazilian government.

The nomination of the ANPD directors is done by the president of the republic and further approved by the Federal Senate¹⁰⁰. This nomination must follow specific rules, especially in relation to the expertise of the person to be nominated and their possible previous relationships with political parties, for example¹⁰¹. Other staff members of the authority are nominated via official procedures considering the hierarchy and organisation of the public entity.

Nominated directors form a regulatory body, which is responsible for deciding specific cases and developing the internal rules of the authority. The ANPD also has a consulting body, the National Council for Data Protection and Privacy (*Conselho Nacional de Proteção de Dados Pessoais e da Privacidade* – CNPD, in the Portuguese acronym). The consultancy body is composed of 23 stakeholders representing different societal sectors¹⁰². The CNPD is responsible for providing non-binding inputs for the National Policy on Data Protection and Privacy and for the activities performed by the ANPD. The Council should also work on the elaboration of studies and public debates about data protection and privacy and on the dissemination of these topics.

Having only been constituted at the end of 2020, the ANPD is still a new structure. According to a national expert, considering that data protection is a relatively recent topic of concern in Brazil (the first discussions on the LGPD began in 2010), the federal administration did not have adequate structures for the development of the ANPD. In recent years, the ANPD has focused many efforts on its regulatory agenda and on establishing basic guidelines for the correct understanding and application of the LGPD. This period was also important for it to structure itself internally and create the necessary formal procedures for law enforcement. Gradually the authority increased its personnel from five presidents and five permanent staff to a hundred permanent staff and twenty temporary staff.

Publishing activity reports is also one of the obligations set by the LGPD to the ANPD (Article 55-J, XII LGPD). So far, the authority has published biannual regulatory agendas and reports on the development of the planned actions to comply with said provision. The topics foreseen in the regulatory agenda for 2021-2022 were all at least initiated¹⁰³. Considering the ongoing aspects of these activities, some topics are also fixed in the new regulatory agenda for 2023-2024 (e.g., international data transfers)¹⁰⁴. Another activity that has just started is the Evaluation of Regulatory Results (*Avaliação de Resultados Regulatórios* – ARR, in the Portuguese acronym). This procedure will allow the ANPD to understand the results of the regulatory activities developed by the authority¹⁰⁵. For now, two topics are

⁹⁹ Autoridade Nacional de Proteção de Dados, *ANPD e Ministério da Justiça e Segurança Pública editam portaria conjunta*, 13 February 2023, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-ministerio-da-justica-e-seguranca-publica-editam-portaria-conjunta>.

¹⁰⁰ Article 5º, Law 9,986/00 (*Lei nº 9.986, de 18 de Julho de 2000, Dispõe sobre a gestão de recursos humanos das Agências Reguladoras e dá outras providências*, available at: http://www.planalto.gov.br/ccivil_03/leis/l9986.htm), and Article 55-D, LGPD.

¹⁰¹ Article 8º-A and 8º-B, Law 9, 986/00.

¹⁰² The ANPD received 120 names for composing the CNPD (Grossman, L. O., ‘ANPD recebeu 120 indicações para Conselho Nacional de Proteção de Dados’, *Convergência Digital*, 26 March 2021, available at: <https://www.convergenciadigital.com.br/Seguranca/ANPD-recebeu-120-indicacoes-para-Conselho-Nacional-de-Protecao-de-Dados-56510.html?UserActiveTemplate=site>).

¹⁰³ Autoridade Nacional de Proteção de Dados, *ANPD divulga balanço de acompanhamento e execução da Agenda Regulatória 2021/2022 referente ao 2º semestre de 2022*, 16 January 2023, available at:

<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga->, available at: [balanco-semestral-de-acompanhamento-e-execucao-da-agenda-regulatoria-2021-2022](https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-).

¹⁰⁴ Autoridade Nacional de Proteção de Dados, *Portaria ANPD n. 35, de 4 de novembro de 2022, Agenda Regulatória para o biênio 2023-2024*, available at: <https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885>.

¹⁰⁵ Autoridade Nacional de Proteção de Dados, *ANPD publica Agenda de Avaliação de Resultados Regulatórios*, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-de-avaliacao-de-resultados-regulatorios>.

going through this assessment: regulation on the procedure of oversight by the ANPD, and regulation on dosimetry of sanctions¹⁰⁶.

2.1.6 TRANSPARENCY RULES IN THE PUBLIC SECTOR

Publicity and transparency are essential principles that guarantee the democratic control of state activities. In Brazil, the Access to Public Information Law (*Lei de Acesso à Informação* – LAI in the Portuguese acronym) applies to the executive, legislative and judicial branches and public authorities of the Federal, State, Municipal and Federal District levels, as well as to private entities that receive public funding to carry out activities in the public interest. The protection of classified and personal information should be observed by every actor to whom the LAI applies, guaranteeing the availability, authenticity, integrity, and restrictions of access to this information.

Since the LGPD entered into force, various requests of data access based on LAI have been denied often unjustifiably¹⁰⁷. However, these two legal instruments are compatible and should be observed in parallel. The current understanding of the ANPD on the application of the ‘compliance with a legal or regulatory obligation’ legal basis should be applied in these cases. Once it is legally mandatory for an information to be made publicly available, the LGPD should not be understood as an obstacle to prevent such publication, but as a set of criteria to balance the fulfilment of different human rights¹⁰⁸.

Public authorities must also carry out a case-by-case analysis of the application of both laws. Recently, the ANPD issued a specific opinion in one of these cases. In February 2022, the National Institute of Educational Studies and Research Anísio Teixeira (*Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira* – INEP in the Portuguese acronym) understood that the disclosure of data contained in the publications of the National Examination of Secondary Education (*Exame Nacional do Ensino Médio* – ENEM in the Portuguese acronym) 2020 and the Basic Education School Census (Censo Escolar da Educação Básica) 2021 could risk identifying students and violate their right to data protection. The data are generally used to inform research and public education policies. The ANPD's opinion for this case was that the institute should prepare a Data Protection Impact Assessment, to assess the risks that may be caused to data subjects with the data disclosure. The report must be made public, where applicable, in order to provide transparency to the decisions and measures that will be adopted by the institute. In addition, the ANPD understood that the INEP is in a position to decide on the extent of the disclosure, and it is possible that microdata be presented in different versions for society and for research institutions, through a term of responsibility¹⁰⁹.

The Brazilian Office of the Controller General (*Controladoria Geral da União* – CGU in the Portuguese acronym) is the competent authority to oversee the LAI application in the federal government. Considering the necessity of clarifying the co-existence of data protection and access rules, the CGU and the ANPD recently signed a cooperation agreement¹¹⁰.

¹⁰⁶ Autoridade Nacional de Proteção de Dados, *Resolução CD/ANPD n. 5, de 13 de março de 2023, Agenda de Avaliação de Resultado Regulatório para o período 2023-2026*, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-de-avaliacao-de-resultados-regulatorios/RESOLUON5ARR.pdf>.

¹⁰⁷ A report published in 2022 evaluated that at least one of four LAI requests that the federal government denied because of the LGPD were not lawful (Fiquem Sabendo, INSPER, FGV, *Impactos da LGPD nos pedidos de LAI ao governo federal*, 2022, available at: https://drive.google.com/file/d/1LfYUOjNVxC1LAL3U_fGwWSCNL7t16ap/view).

¹⁰⁸ Bioni, B. R., Silva, P. G. F., Martins, P. B., ‘Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso’, *Cadernos técnicos da CGU: coletânea de artigos da pós-graduação em ouvidoria pública*, 2022, pp. 8–19.

¹⁰⁹ Autoridade Nacional de Proteção de Dados, *ANPD manifesta-se sobre divulgação de microdados do Enem e Censo Escolar pelo INEP*, 17 Mai 2022, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-manifesta-se-sobre-divulgacao-de-microdados-do-enem-e-censo-escolar-pelo-inep>.

¹¹⁰ Controladoria-Geral da União, *CGU e ANPD firmam parceria para cooperação entre os órgãos*, 17 February 2023, available at: <https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/02/cgu-e-anpd-firmam-parceria-para-cooperacao-entre-os-orgaos>.

2.1.7 CYBERSECURITY

Data security is an essential safeguard that should be considered when assessing the proportionality of processing of personal data by the state.

Currently, Brazil ranks 18th in the world on the International Telecommunications Union's Global Cybersecurity Index 2020¹¹¹, which is already a huge improvement from the 2018 edition¹¹², where the country ranked 70th. There are still no specific laws nor bills being discussed in Brazil that deal with cybersecurity in detail. That does not mean, however, that cybersecurity has not been on the national agenda.

In 2018, the Presidential Decree n. 9637¹¹³ instituted the National Information Security Policy within the scope of the federal public administration, providing guidance on information security governance and providing for a waiver of public procurement procedures in cases that could compromise national security. The policy established as instruments of its application the National Information Security Strategy (E-Ciber, explained below) and national plans (which detail the implementation of strategic actions, the planning of activities and the allocation of responsibilities). The Information Security Management Committee was created, with the attribution of advising the Institutional Security Office of the Presidency of the Republic in activities related to information security. The committee is, however, composed only of representatives of the public sector.

In order to provide more clarity in relation to the cybersecurity part of the 2018 National Information Security Policy, the Presidential Decree 10.222 of 2020¹¹⁴ established Brazil's National Cybersecurity Strategy (E-Ciber). It is the “first official document to provide an overview regarding Brazil’s role in cybersecurity, as well as objectives and guiding principles for its development between 2020 and 2023”¹¹⁵. E-Ciber details which strategic actions should be implemented by Federal Administration bodies, according to their specific competencies. Since then, several bodies have begun to formalise their internal information security programmes, which is a great achievement for the country. However, the programmes are still superficial and incapable of guaranteeing efficient coordination between public administration, the private sector and the third sector.¹¹⁶

It is important to mention that the LGPD also provides important provisions related to cybersecurity. Article 6, VII, defines security as one of the principles that should be followed while processing personal data. Chapter VII, Section I, on Security and Data Confidentiality also requires, *i.a.*, that controllers and processors must adopt security, technical and administrative measures to prevent personal data from unauthorised access, as well as accidental or unlawful situations of destruction, loss, alteration, communication or any form of inappropriate or unlawful data processing (Article 46, LGPD). The

¹¹¹ International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI)*, 2020, available at: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>.

¹¹² International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI)*, 2018, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

¹¹³ Decreto nº 9.637, de 26 de Dezembro de 2018, Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional, available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm#:~:text=DECRETO%20N%C2%BA%209.637%2C%20DE%202026,regulamenta%20o%20disposto%20no%20art.

¹¹⁴ Decreto nº 10.222, de 5 de fevereiro de 2020, Aprova a Estratégia Nacional de Segurança Cibernética, Brasil, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

¹¹⁵ Hurel, L. M., *Cybersecurity in Brazil: An analysis of the National Strategy*, Igarapé Institute, 2021, available at: https://igarape.org.br/wp-content/uploads/2021/04/SP-54_Cybersecurity-in-Brazil.pdf.

¹¹⁶ See Belli, L. et al, *Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil digitalmente soberano*, 2023, available at: <https://cyberbrics.info/ciberseguranca-uma-visao-sistematica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/>, for a detailed analysis of the current application of E-Ciber and other federal policies.

ANPD may also provide minimum technical standards for this purpose (Article 46, paragraph 1º, LGPD).

2.1.8 PUBLIC SECURITY

Brazil experiences many public security issues. For example, police brutality in Brazil is a point of attention. Although reliable figures on killings by police are hard to find, since governments often do not collect or publish them¹¹⁷, the Brazilian police is known to be one of the most lethal in the world, with more than 6 100 deaths in 2021, or 17 per day on average¹¹⁸. In 2022, following a police raid that killed 23 people in a favela in Rio de Janeiro, “UN experts called on the Brazilian Government to adopt wide-ranging reforms to put an end to police violence, demilitarise all law enforcement agencies and vigorously address systemic racism and racial discrimination”¹¹⁹.

Technologies are then seen by many as a way not only to bring more efficiency to the work of the security forces, but also to insert certain neutrality and remove discriminatory biases, especially racial discrimination¹²⁰. In a recent survey carried out by the Fundação Getúlio Vargas, the most used technologies by Brazilian security forces are drones (63 %), Optical Character Recognition technologies, mainly used to identify number plates (44 %); facial recognition, (33 %), cameras attached to police uniforms (22 %) and predictive policing technologies (7 %)¹²¹.

The LGPD does not fully apply to public security activities and clear and up-to-date rules on the use of data for this purpose do not yet exist. A future data protection law for public security and criminal prosecution will have to provide for proportionate and strictly necessary measures for fulfilling the public interest, subject to due legal process, and observe the general principles of protection and the rights of the data subject (Article 4(1) LGPD). This is further discussed in more detail in section 2.2 below.

In Brazil, the competence to deal with public security is shared between different levels of the federation and encompasses different bodies, which makes a unique analysis of the use of personal data by these institutions a complex task. According to Article 144, Constitution, public security is a duty of the State and a right and responsibility of all. It is exercised for the preservation of public order and the safety of people and property, through the following bodies: federal police, federal road police, federal railway police, civilian police, military police and military fire departments, and federal, state and district criminal police. Municipalities mainly play a role in prevention, although the expansion of the municipal guard forces has included repression tasks¹²².

External control of institutions responsible for public security is carried out by different bodies, depending on the sphere of government and the type of institution. In general, they are controlled by the Public Prosecutor's Office, whether state or federal (Article 129, VII, Constitution). This constitutional provision is detailed in specific laws of each state and, within the federal scope, in the Complementary Law N° 75/1993, which provides for the organisation, attributions and statute of the Federal Public

¹¹⁷ Amnesty International, *Police Violence*, available at: <https://www.amnesty.org/en/what-we-do/police-brutality/>.

¹¹⁸ Le Temps, *Une opération policière dans une favela de Rio fait au moins 22 morts*, 24 May 2022, available at: <https://www.letemps.ch/monde/ameriques/une-operation-policiere-une-favela-rio-22-morts>.

¹¹⁹ United Nations, *Brazil: UN experts decry acts of racialised police brutality*, 6 July 2022, available at: <https://www.ohchr.org/en/press-releases/2022/07/brazil-un-experts-decrys-racialised-police-brutality>.

¹²⁰ According to Amnesty International, racism in Brazil continues to drive state violence, “Mass killings by public security officials were frequent, disproportionately affecting Black people in marginalized neighbourhoods” (Amnesty International, *Amnesty International Report 2022/23: The State of the World's Human Rights*, 2023, available at: <https://www.amnesty.org/en/location/americas/south-america/brazil/report-brazil>).

¹²¹ Campos, A. C., ‘Drones são adotados por 63% das forças de segurança no Brasil’, *Agência Brasil*, 29 March 2023, available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2023-03/drones-sao-adoptados-por-63-das-forcas-de-seguranca-no-brasil>.

¹²² Cano, I. ‘Public Security Policies in Brazil: Attempts to Modernize and Democratize versus the War on Crime’, *Sur*, No 5, year 3, 2006, available at: <https://sur.conectas.org/en/public-security-polices-brazil/>.

Prosecutor's Office¹²³. This external control by the Public Prosecutor's Office takes place, for example, through the control of police occurrences and their consequences, the professionalisation of inter-institutional relations, the statistical study of the activity of the judicial police, and the training of its members¹²⁴.

Other important oversight bodies include the Judiciary, Ombudsman offices and Police Internal Affairs. The objective of the latter is to monitor and investigate the actions and/or omissions by police officers that involve a breach of the law or of the rules of conduct of the corporation¹²⁵.

2.2 GOVERNMENT ACCESS TO PERSONAL DATA

2.2.1 KEY CONSIDERATIONS

According to Brazilian case law and doctrine, no fundamental right is absolute. As a result, all fundamental rights, including data protection, can be limited depending on the circumstances. Activities of public authorities that limit the right to privacy and to the protection of personal data should always be carried out for the fulfilment of its public purpose, in pursuit of the public interest, and with the objective of executing the legal competences or fulfilling the legal attributions of the public service (Article 23 LGPD). The evaluation of public interest is essential for assessing the proportionality of the interference. The Brazilian Constitution also establishes the legality principle for all actions of the public administration, so any interference to fundamental rights should be conveyed by law (Article 37).

Moreover, Article 50, Federal Administrative Procedures Law¹²⁶, determines that every administrative act must be motivated when they deny, mitigate, or affect rights or interests of citizens. Any measure that limits the protection of personal data should be motivated, but there are no clear general rules on how this motivation should be publicised and scrutinised.

In relation to the interference with the rights to privacy and to the protection of personal data, the LGPD establishes some important safeguards, since it also applies to public authorities. Indeed, public authorities may need to access data for many different reasons, but in addition to a legal basis for data processing, this must be carried out for specific purposes, in a transparent manner, ensuring accountability and the exercise of data subjects' rights. The ANPD can also request that public entities publish their data protection impact assessments as well as adopt specific standards and good practices.

Despite the current need for compliance with the LGPD and the right to data protection being enshrined in the Brazilian Constitution, the use of surveillance technologies in the country has grown steadily since 2006. Between 2012 and 2014, various different systems were trialled in Brazil due to the mega-events held by the country. In 2018, technologies such as facial recognition began to spread in Brazil¹²⁷. The

¹²³Lei Complementar nº 75, de 20 de maio de 1993, Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União, available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp75.htm.

¹²⁴ Conselho Nacional dos Procuradores-Gerais, *Manual Nacional do Controle Externo da Atividade Policial*, 2009, available at:

http://www.mpsp.mp.br/portal/page/portal/cao_criminal/CAOCri_ControleExtAtivPol/Manual%20Nacional%20do%20Controle%20Externo%20da%20Atividade%20Policial.pdf.

¹²⁵ Pereira, A. B. C., Cabral, S., Reis, P. R. da C., 'Accountability interna em forças policiais: explorando os fatores associados ao desempenho de uma corregedoria de polícia militar'. *Organizações & Sociedade*, 27(92), 2020, available at: <https://doi.org/10.1590/1984-9270922>.

¹²⁶Lei nº 9.784, de 29 de Janeiro de 1999, Regula o processo administrativo no âmbito da Administração Pública Federal, available at:

http://www.planalto.gov.br/ccivil_03/leis/l9784.htm#:~:text=LEI%20N%C2%BA%209.784%20%2C%20DE%2029%20DE%20JANEIRO%20DE%201999.&text=Regula%20o%20processo%20administrativo%20n%C2%A0o%20C3%A2mbito%20da%20Administra%C3%A7%C3%A3o%20P%C3%ABlica%20Federal.

¹²⁷ Instituto Igarapé, *Reconhecimento Facial no Brasil*, available at: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>.

peak of implementation of these technologies in 2020 was mainly due to the surveillance projects developed during the pandemic. In a recent report on the use of surveillance technologies in Brazil, it was identified that the majority of them (76.4 %) were implemented for purposes of public security, but they were also found in areas such as health, tourism and economy¹²⁸.

2.2.2 NATIONAL SYSTEM OF INTELLIGENCE

The Brazilian Intelligence System (*Sistema Brasileiro de Inteligência* – SBI in the Portuguese acronym) was established by Law n. 9,883/99¹²⁹, which created the Brazilian Agency of Intelligence (Agência Brasileira de Inteligência – ABIN in the Portuguese acronym). The law determines that only public authorities that are part of this system may produce knowledge of interest to the nation, according to the Presidential Act (Article 2º, Law n. 9,883/99)¹³⁰.

All public authorities' part of the intelligence system must comply with all constitutional provisions, including fundamental rights and freedoms, international conventions, agreements and adjustments, as well as other legislation. This should be considered during the performance of their duties, which include the processing of information needed for the executive power decision making. The processing of data must also protect the information against the access of non-authorised persons or bodies.

The acts of the Executive Power are overseen by the National Congress and the Federal Court of Accounts (*Tribunal de Contas da União* - TCU in the Portuguese acronym) (Article 49, X, Brazilian Constitution)¹³¹ and any violation of rights can be brought to the judicial power (Article 5, XXXV, Brazilian Constitution). Thus, any issue regarding data usage may be evaluated by the legislative or judiciary powers. Any of these decisions are binding and should follow due process.

ABIN is the central body of the system, which is responsible for planning, executing, coordinating, supervising, and overseeing the intelligence activities. These activities must be carried out using confidential means and techniques. To comply with all its duties, ABIN must receive specific knowledge and data related to the defence of institutions and national interests from the different public authorities part of the SBI (Article 4, Law n. 9,883/99).

In a recent STF decision, the lawfulness of this article was questioned¹³². The ruling stated that the data that public authorities share with ABIN must abide by all formal rules, observing the strict public interest (defence of public institutions and national interest). In case of non-compliance, the activity should be declared unlawful by the judiciary. To guarantee this oversight procedure, it is essential that the purpose of each data sharing activity is defined through formal procedures. This information should be publicly available together with information on how this processing complies with the legal requirements.

Any data sharing activity must also take place on electronic systems with security and data access control, to facilitate oversight. This allows the judiciary to assess if there is a lawful public interest for the processing activities, if the competences are not overlapping (e.g., ABIN has no competence of accessing data collected by waiving of telephone communication secrecy or other data that can only be

¹²⁸ Instituto Igarapé, *Implementação de Tecnologias de Vigilância no Brasil e na América Latina*, 2022, available at: <https://igarape.org.br/wp-content/uploads/2022/12/Implementacao-de-tecnologias-de-vigilancia-no-brasil-e-na-america-latina.pdf>.

¹²⁹ Lei nº 9.883, de 7 de Dezembro de 1999, Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências, available at: https://www.planalto.gov.br/ccivil_03/leis/19883.htm.

¹³⁰ Decreto n. 4376/02 provides more detail on the organisation and functioning of the SBI (Decreto nº 4.376, de 13 de Setembro de 2022, Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999, e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/decreto/2002/d4376.htm).

¹³¹ The oversight activities can be developed by other bodies that collaborate with the National Congress, such as the Federal Court of Accounts (*Tribunal de Contas da União* – TCU in the Portuguese acronym).

¹³² Supremo Tribunal Federal, *STF confirma limitações ao compartilhamento de dados do Sisbin*, 15 October 2021, available at: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=474835&ori=1>.

accessed upon a judicial decision), and evaluate if there were any omissions, misapplications, or abuses, which may lead to the liability of agents and/or bodies¹³³. In light of the general binding effect of STF decisions, data processing activities carried out by intelligence agencies should all observe this decision. Beyond the internal oversight provided by the ABIN, it is important to note that the ANPD can also carry out audits in the intelligence bodies.

The legal framework provides for an effective oversight of intelligence activities in Brazil. In recent news pieces, it was suggested that the previous federal government used an ABIN system to monitor individuals, gathering information on the location of the citizens via their cell phones. These activities are being investigated by the Federal Police, the National Congress and the TCU.
[REDACTED]

During the last years, various scandals involving the intelligence system and the federal government were reported in Brazilian news outlets,
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Contracts signed by the Executive Power are overseen by the Legislative power, especially by the TCU. Thus, the engagement between the ANPD and the TCU seems like a good initiative to guarantee data protection even in cases involving intelligence or national security activities. For instance, a procedure finalised by the TCU in 2022 evaluated the acquisition of a surveillance system to be used in open data sources. The decision allowed the intelligence entities to move on with the contract but also determined the notification of the ANPD to guarantee further oversight¹³⁷.

2.2.3 CRIMINAL PROSECUTION

As mentioned above, the LGPD does not fully apply to certain circumstances, such as when data are processed for purposes of public security, national defence, State security, or investigation and repression of criminal offences (Article 4º, III LGPD). The LGPD demands that a dedicated law be issued to deal with these situations. In relation to two of them, public security and criminal prosecution, a working group was created in 2019 by the Brazilian National Congress to prepare a bill.

The “Draft Data Protection Law for public security and criminal prosecution”¹³⁸ was presented to Congress by the commission in December 2020. However, the proposal did not move in view of the need for a parliamentarian to adopt it and take it forward in the legislative process¹³⁹. With this situation,

¹³³ Supremo Tribunal Federal, ADI 6529, 2021, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837>
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

¹³⁷ Tribunal de Contas da União, Processo n. 014.760/2021-5, 2022.

¹³⁸ Câmara dos Deputados do Brasil, *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*, 2019, available at: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf>.

¹³⁹ Although the draft bill itself was not adopted by any parliamentarian, a national expert explained that several bills have emerged in recent years with a very similar structure to the working group’s proposal. The most discussed bill adopts almost all the suggestions of the working group, but excludes the majority of data subjects rights (Câmara dos Deputados, PL 1515/2022, available at: <https://www.camara.leg.br/propostas-legislativas/2326300>).

there is still relative legal uncertainty; however, the LGPD is clear in establishing that further specific regulation for these exceptions must provide for proportional and strictly necessary measures for fulfilling the public interest, subject to due legal process, and observe the general principles of protection and the rights of the data subject (Article 4, paragraph 1º, LGPD). Thus, national experts are of the opinion that the principles of data protection must already be observed for these activities. The recent recognition of the fundamental right to the protection of personal data by the Brazilian constitution also reinforces the need for minimal safeguards for any processing of personal data in the country.

A Brazilian non-binding norm¹⁴⁰ also determines that the processing of personal data for the purpose of national security, public security, national defence, and criminal procedures should follow due process, the general principles of data protection and the data subjects' rights established in the LGPD. Although non-binding, this kind of interpretive statement is often used as guidance by the Brazilian judiciary.

It is important to mention that although this specific law still does not exist, there are some rules that apply to data processing for criminal prosecution in Brazil. The confidentiality of correspondence of electronic and telephone communications is considered as a fundamental right in the Brazilian legal framework. Public authorities can access these data only in exceptional cases for the purposes of criminal investigations or prosecution. Therefore, the interception of communication must always be a subsidiary and exceptional measure, that is only allowed when there are no other means to solve a specific case¹⁴¹. Furthermore, Article 2 of the Telephone Interception Law provides that the interception of telephone communications shall not be accepted in any of the following circumstances: (i) there is no reasonable evidence of authorship or participation in a criminal offence; (ii) the proof can be provided by other available means; (iii) the fact investigated constitutes a criminal offence punishable only by detention, i.e. the offence is not punishable by the more severe penalty of imprisonment¹⁴². In any case, the request for telephone interception must clearly describe the situation under investigation, including the identification and qualification of those investigated, unless this is manifestly impossible, which should be duly justified.

The procedural safeguards in case of an interception of communication can only be set out in federal legislation. In that regard, the Telephone Interception Law requires a judicial ruling, by motion of a court, by the court that hears a particular case, by police authorities during criminal investigations, or by the public prosecutor, during the investigation or the prosecution (Article 3º). In any case, the request for interception must clarify the necessity of the measure (Article paragraph 4º). The authorisation will lead to access the content of the communications and is valid for 15 days. This period can be extended by a new decision, once the indispensability of the measure is proven, and there is no limit on how often such a new decision can be requested (Article 5º)¹⁴³. The law reaffirms the exceptionality of the interception, establishing the obligation for the Court to verify the proportionality of the measure (Article paragraph 2º).

Although in general a judicial ruling is necessary to have access to telecommunication data, there are some exceptions. The Brazilian Criminal Procedure Code¹⁴⁴, in its Article 13-A, determines that during

¹⁴⁰ Conselho da Justiça Federal, IX Jornada de Direito Civil, Enunciado 678, 2022, available at: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf/view>. Enunciados are texts proposed by the public and accepted by a committee set by a Court that will provide guidance to the Judiciary.

¹⁴¹ Supremo Tribunal Federal, HC 108147/PR, 2012, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401>.

¹⁴² Lei nº 9.296, de 24 de Julho de 1996, Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, http://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

¹⁴³ Supremo Tribunal Federal, HC 133148/ES, 2017, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4932933>.

¹⁴⁴ Decreto-Lei nº 3.689, de 3 de Outubro de 1941, Código de Processo Penal, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

the investigation of some crimes¹⁴⁵, members of the Public Prosecutor's Office or the police chief may request, from any government agency or private company, registration data related to victims or suspects.

Another exception is found in Article 13-B of the Brazilian Criminal Procedure Code. If necessary for the prevention and repression of crimes related to human trafficking, the member of the Public Prosecutor's Office or the police chief may request, upon judicial authorisation, the companies providing telecommunications and/or telematics services to immediately make available the appropriate technical means – such as signs, information and others – that allow locating the victim or suspects of the ongoing crime. Judicial authorisation will depend on the conditions for access provided by the Brazilian Constitution, as outlined above, and in particular on whether such access is a subsidiary and exceptional measure¹⁴⁶. If there is no judicial manifestation within twelve hours, the competent authority will request the companies providing telecommunications and/or telematics services to immediately make available the appropriate technical means, with immediate communication to the judge.

As a rule, the implementation of the interception measure is an activity undertaken by the police. However, it is possible that specialised services or other public authorities get involved in the procedure to guarantee the due execution of the measure. In such cases, they will have to follow the applicable legal framework. Involving other entities will only take place to guarantee the safety and efficiency of the measure, but should always respect the need of a judicial decision¹⁴⁷. The result of the interception must be sent to the competent court, which stores the data in separate files to guarantee the secrecy of the communications (Article 8º). Nonetheless, the STF ruled that when the outcome of the interception is not stored in separate files, this amounts to a mere irregularity and does not entail the nullity of the interception¹⁴⁸ as long as it follows the legal procedure. Not following the legal provisions and obligations leads to the complete nullity of the interception. This means that the information must be excluded of the proceedings by motion of the prosecution or the interested party (Article 9º). This information must also not be used in other procedures¹⁴⁹.

Also, according to the Telephone Interception Law, a judicial order can authorise the recording of a specific environment or the capture of electronic, optical, or acoustic signals by a motion of the police authority or the Public Prosecutor. According to these procedures, interception without a judicial authorisation or for the purpose of unlawful activities constitutes a crime (Article 10).

The result of the interception may be used as evidence in other procedures – even administrative ones – and in the prosecution of other crimes. For instance, if the interception leads to the discovery of another crime, the results can be used as evidence even if the crime is not related to the one being initially investigated¹⁵⁰. There are limits on using the interception results for another investigation procedure when the person involved in the new crime has privileged jurisdiction and the measure was authorised

¹⁴⁵ The exhaustive list of rights are: kidnapping and false imprisonment (Article 148), reduction to a condition analogous to slavery (Article 149), human trafficking (Article 149-A), extortion by restricting the victim's freedom (Article 158, paragraph 3º) and extortion by kidnapping (Article 159), in the Criminal Code (*Decreto-Lei nº 2.848, de 7 de Dezembro de 1940, Código Penal*, available at: http://www.planalto.gov.br/ccivil_03/decreto-.available.at:lei/del2848compilado.htm), and children trafficking (Article 239), in the Child and Adolescent Statute (*Lei nº 8.069, de 13 de Julho de 1990, Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências*, available at: http://www.planalto.gov.br/ccivil_03/leis/18069.htm).

¹⁴⁶ Supremo Tribunal Federal, HC 108147/PR, 2012, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401>.

¹⁴⁷ See Supremo Tribunal Federal, HC 96986/MG, 2012, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=2649995>. For instance, in this case, other police bodies were involved in the interception, since there were doubts about the involvement of police officers in the crime analysed.

¹⁴⁸ Supremo Tribunal Federal, HC 128102/SP, 2015, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4770762>.

¹⁴⁹ Supremo Tribunal Federal, ARE 1316369/DF, 2022, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6129951>.

¹⁵⁰ Supremo Tribunal Federal, HC 129678/SP, 2018, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4820467>.

by a non-competent judge¹⁵¹. However, in regular cases, even interceptions authorised by different Courts can lead to evidence that can be used for the investigation of other crimes¹⁵². The main point is having the legal procedure followed, guaranteeing the rule of law and due process.

The waiving of telephone communication secrecy can also be requested by a federal or state Parliamentary Investigation Committee (*Comissão Parlamentar de Inquérito* – CPI in the Portuguese acronym), leading to the access of telecommunication metadata, which cannot be made publicly available¹⁵³. The CPI is a procedure used by the National Congress to exercise its oversight powers. The CPI cannot judge or punish the ones being investigated, and cannot determine the interception of communications by itself — a court order is still necessary in this case.

It is important to highlight that the STF's, as well as the Brazilian Superior Tribunal of Justice (STJ)'s case law state that the constitutional protection of telecommunication data encompasses the mere data communication flow and not the data themselves. They have ruled that accessing the content of e-mails or private conversations retained in electronic devices that were gathered as evidence by investigation authorities, for instance, is allowed and a specific judicial order is not needed. For instance, if there is a judicial decision for search and seizure, the seized electronic equipment can be accessed by the investigation bodies¹⁵⁴.

In terms of investigation activities, one national expert explained that in the current national legal framework, no default classification is applied to data. However, considering that some case files might contain sensitive information or classified data (e.g., bank secrecy, attorney-client information), there might be some access limitations. There are no specific rules determining that the data subjects must be informed of the processing of their personal data. If the data subject is part of the criminal procedure (e.g., as a victim, suspect, or witness), the individual will be invited to provide information for the investigation. In this case, the data subject will know that their data are being processed. However, if a person is not invited to take part in the procedure, they will most probably not know that their personal data was processed.

On the international level, Brazil has been a signatory of the Budapest Convention since 2021, which was implemented in the Brazilian Legal System through the Legislative Decree n. 37/2021¹⁵⁵. Although the first protocol is already in force, a working group of national experts are still discussing how to implement the second one. The signing of the Convention was highly celebrated by government authorities and the private sector. However, the process raised many concerns in Brazilian civil society such as the approval of the Convention in a shorter period than expected and without multistakeholder discussions on the subject; the absence of a general data protection law dedicated to criminal prosecution and public security activities; and the fact that the Convention was approved during the recast discussions of the Brazilian Criminal Procedure Code, which contains dedicated provisions regulating online investigation activities, data collection and cooperation between companies and public authorities¹⁵⁶. A national expert stated that it is currently not possible to assess how the convention is being internalised by public authorities. Under the current government, the central authority for the oversight of the Convention is the Department of Asset Recovery and International Cooperation

¹⁵¹ Supremo Tribunal Federal, MS 34751/CE, 2018, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5172309>.

¹⁵² Superior Tribunal de Justiça, REsp 1355432-SP, 2014, available at:
https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201202488103.

¹⁵³ Supremo Tribunal Federal, MS 25940, 2018, <https://portal.stf.jus.br/processos/detalhe.asp?incidente=2376827>.

¹⁵⁴ Superior Tribunal de Justiça, RHC 75800/PR, 2016, available at:
<https://processo.stj.jus.br/webstj/Processo/justica/jurisprudencia.asp?valor=201602394838>.

Supremo Tribunal Federal, RHC 132062/RS, 2016, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4903009>.

¹⁵⁵ Decreto Legislativo nº 37 de 16 de Dezembro de 2021, Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, available at: <https://legis.senado.leg.br/norma/35289207>.

¹⁵⁶ Santos, B. M., *Convenção de Budapeste Sobre o Cibercrime na América Latina: uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México*, Derechos Digitales, 2022, available at:
<https://www.derechosdigitales.org/wp-content/uploads/PT-Ciberdelincuencia-2022.pdf>, p. 21.

(Departamento de Recuperação de Ativos e Cooperação Internacional - DRCI in the Portuguese acronym), part of the Ministry of Justice and Public Safety¹⁵⁷.

Another important development related to international cooperation in the criminal field is the STF ruling that took place in February 2023 on the constitutionality of the Mutual Legal Assistance Treaty (MLAT) between Brazil and the United States¹⁵⁸. Although the ruling confirmed the constitutionality of Decree n. 3,810/2001, which enacted the treaty, the STF understood that national authorities can request data directly from platforms based abroad¹⁵⁹. According to the treaty, data requests should be intermediated by the Ministry of Justice and Public Safety, but the Court understood that the Brazilian judiciary can use other resources to obtain information from providers, such as direct subpoenas from companies in Brazil or rogatory letters, under the terms of Article 11, MCI. The rapporteur of the case, Justice ██████████, highlighted the low effectiveness of the cases that used the procedure established in the MLAT. He determined that the STF must inform the Legislative and Executive powers of the decision so that they can take action in relation to the discussions on the Data Protection Law for public security and criminal prosecution and new bilateral or multilateral agreements. ██████████ also highlighted that the MLAT rule should be adopted in a complementary way and only when it is impossible for national authorities to directly obtain information from digital platforms.

2.2.4 DATA SHARING

The Presidential Decree n. 10,046/19 sets rules on data governance and the sharing of personal data within the federal public authorities and establishes the *Cadastro Base Cidadão* (central national identification data base) and the Central Committee of Data Governance. The Decree's rules do not apply to situations where data is shared with supervisory boards for regulated professions and with the private sector as well as to data protected by fiscal secrecy under the control of the Ministry of Economy. However, it does apply to the remaining federal public authorities.

There are three possible levels of data sharing depending on the data classification: (i) broad, involving public data (Article 11); (ii) restrict, involving classified data but that are accessible by all public authorities that should follow the Decree (Article 12); and (iii) specific, also affecting classified data, but with public authorities having limited and specific access to the information (Article 14). New data bases can only be created when the possibilities of exploring existing ones are not enough (Article 10-A).

In view of the legal nature of the decree, it cannot be interpreted as amending or derogating from the LGPD. However, since its enactment, the decree has been criticised by many actors in Brazilian Civil Society, for not aligning with the LGPD¹⁶⁰. Generally speaking, the decree does not consider the need for a legal basis for access to personal data by public bodies (and not only the data sharing); does not require the need to specify the purposes for which the data will be shared and with whom (which directly

¹⁵⁷ Vassallo, L., Kattah, E., Medeiros, D., ‘Governo Lula vai rever cooperação do MPF com outros países; medica foi central na Lava Jato’, *Estadão*, available at: <https://www.estadao.com.br/politica/governo-lula-vai-rever-cooperacao-do-mpf-com-outros-paises-medida-foi-central-na-lava-jato/>.

¹⁵⁸ Supremo Tribunal Federal, ADC 51, 2023, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>.

¹⁵⁹ Maia, F., ‘STF: MLAT é constitucional, mas acordo não é a única forma de obtenção e prova’, *Jota*, 23 February 2023, available at: <https://www.jota.info/stf/do-supremo/stf-mlat-e-constitucional-mas-acordo-nao-e-a-unica-forma-de-obtencao-de-prova-23022023>.

¹⁶⁰ Associação Data Privacy Brasil de Pesquisa, *Intervenção como amicus curiae - Ação Direta de Inconstitucionalidade nº 6.649*, available at: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755538665&prcID=6079238>; Laboratório de Pesquisa em Políticas Públicas e Internet (LAPIN), *Nota Técnica - Derrubada dos Decretos 10.046/2019 e 10.047/2019 - Compartilhamento de dados no âmbito da administração pública federal*, available at: <https://lapin.org.br/wp-content/uploads/2020/08/NT.-2-Derrubada-dos-Decretos-10.0462019-e-10.0472019.-LAPIN.pdf>.

affects the analysis of necessity and proportionality); does not provide for traceability mechanisms, such as agreements or terms of authorisation; and does not allow the exercise of data subjects' rights.¹⁶¹

In September 2022, the STF ruled on two cases that focused on the indiscriminate data sharing in the Federal Public Administration, authorised by Decree n. 10,046/2019¹⁶². One of them discussed the situation where data from 76 million Brazilians from the National Traffic Department (*Departamento Nacional de Trânsito - DENATRAN*, in the acronym in Portuguese) would be shared with ABIN. In this opportunity, the Court clarified that the LGPD must be applied to data sharing within the scope of the decree. Thus, there are limits to the onward sharing of personal data between public entities. Negligent and abusive acts regarding the processing of personal data by public authorities are submitted to further liability procedures.

The Court also decided that data sharing within the scope of intelligence activities must observe specific legislation and parameters established in the ruling of ADI 6529, already mentioned above, and meet the public interest. Finally, the ruling declared the unconstitutionality of Article 22 of the decree, which organised the structure of the Central Data Governance Committee. The court granted 60 days for the public administration to adjust the composition of the committee, providing it with a plural and independent composition, in addition to creating rules for the accountability of infringing agents. This was complied with by Decree n. 11,266/2022.

2.2.5 OVERSIGHT MECHANISMS

The ANPD is the central body responsible for providing guidance on the interpretation and oversight of data protection rules (Article 55-K, sole paragraph and Article 55-J, XX, LGPD). The authority also holds the exclusive competence of applying administrative sanctions in such cases (Article 55-K, LGPD). Sanctions foreseen by the LGPD include powers to ensure compliance with data protection rules (e.g., binding orders of erasure of data basis, publishing the infraction) and pecuniary fines, as explained above.

The ANPD is also competent to request information regarding the processing of data by a public body, which may include audits over the processing of personal data held by it¹⁶³. Even though the ANPD has limited oversight powers in the activities out of the scope of the law, the authority can request information to public bodies involved in such tasks, including data protection impact assessments. The ANPD can also publish opinions and recommendations for guaranteeing best practices of data protection for all kinds of data processing activities.

The oversight of activities out of the scope of the LGPD also involve the judicial supervision foreseen for surveillance activities such as interception of communications. As mentioned before, other bodies are also engaged in control activities, especially the TCU and the CGU.

The Brazilian system also allows the ANPD to apply sanctions to public bodies within the scope of LGPD, except for fines that can only be applied to private entities¹⁶⁴. As a rule, for oversight purposes, the public body should be considered as the controller or processor, not a specific civil servant. However,

¹⁶¹ Mendes, L. M., Gasiola, G. G., 'Inconstitucionalidade do Decreto 10.046: limites do compartilhamento de dados', *Conjur*, 14 September 2022, available at: <https://www.conjur.com.br/2022-set-14/schertel-gasiola-compartilhamento-dados-setor-publico>; Mendes, L. S., 'Laura Schertel Mendes: Democracia, poder informacional e vigilância', *OGlobo*, 13 August 2022, available at: <https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml>.

¹⁶² Supremo Tribunal Federal, ADI 6649, 2022, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238>, and Supremo Tribunal Federal, ADPF 695/DF, 2022, available at: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693>.

¹⁶³ Article 55-J, XVI, LGPD.

¹⁶⁴ Article 52, paragraph 3º, LGPD.

sanctioning the individual who works in the public administration is possible¹⁶⁵, if their behaviour falls under one of the provisions that would allow for this (e.g., selling data sets or modifying data)¹⁶⁶.

Taking into account that the ANPD is still relatively new, only recently did it announce that it will begin the sanctioning process and that it already has eight ongoing cases that could result in the application of penalties¹⁶⁷. As explained by a national expert, a number of high-profile cases have also been examined since the start of its activities. For example, in a case involving data sharing between two companies providing chat applications [REDACTED], the ANPD worked together with the National Consumer Secretariat (*Secretaria Nacional do Consumidor* – SENACON in the Portuguese acronym), the Administrative Council for Economic Defense (*Conselho Administrativo de Defesa Econômica* – CADE in the Portuguese acronym) and with the Federal Public Prosecutor's Office (*Ministério Público Federal* – MPF in the Portuguese acronym). [REDACTED]

[REDACTED] Another example is the opinion given by the ANPD in the INEP case mentioned above. In recent years the ANPD also signed some important technical cooperation agreements such as with SENACON, CADE and the Superior Electoral Court (*Tribunal Superior Eleitoral* – TSE in the Portuguese acronym) to joint efforts to promote the proper application of the LGPD. Finally, the authority has also worked on a number of requests for advice and guidance issued by public authorities and private entities.

As mentioned throughout the analysis, apart from the ANPD, several other public bodies have competences that are also important to make sure that the public sector complies with the rights to privacy and to the protection of personal data, such as the Prosecutor's Office and the Judiciary. The CGU, for example is the competent authority to oversee the LAI application in the federal government. In the draft bill for the law for public security and criminal prosecution, CGU is also foreseen as the competent authority to oversee the application of the law. In relation to the Budapest Convention, a department within the Ministry of Justice and Public Safety is considered the central authority.

As for intelligence activities, internal control by the executive branch is carried out not only by the hierarchy of each agency, such as the ABIN, but also by the executive ministry to which it is part of. The external control is made by the judiciary and the legislative powers. The judiciary has a prior role, for example, by authorising actions such as telephone interception and breach of telephone communication secrecy. *A posteriori*, it will adjudicate lawsuits from citizens against the intelligence services and those initiated by the Public Ministry. The latter also has its role as a supervisor of the law and instance of external control of the police. Finally, the legislative power has the primary role of supervising the intelligence activities, both directly, through the Joint Commission for Control of Intelligence Activities of the National Congress (*Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional* – CCAI in the Portuguese acronym), and through bodies that report to the Parliament, such as the TCU¹⁶⁹.

¹⁶⁵ Article 28, Decreto Lei 4657/42.

¹⁶⁶ Autoridade Nacional de Proteção de Dados, *Tratamento de Dados Pessoais pelo Poder Público*, 2022, available at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>.

¹⁶⁷ Souza, N. ‘ANPD mira em punições para garantir cumprimento da lei de dados’, *Jota*, 6 February 2023, available at: <https://www.jota.info/coberturas-especiais/protecao-de-dados/anpd-mira-em-punicoes-para-garantir-cumprimento-da-lei-de-dados-06022023>.

[REDACTED]
Beyond the joint statement, the ANPD also issued technical opinions on the matter. (Autoridade Nacional de Proteção de Dados, *Nota Técnica n. 02/2021/CGTP/ANPD*, 2021, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NotaTecnicaANPDWhatsApp_ocr.pdf; Autoridade Nacional de Proteção de Dados, *Nota Técnica n. 19/2021/CGF/ANPD*, 2021, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTecnica19_2021.CGF.ANPD.pdf; Autoridade Nacional de Proteção de Dados, *Nota Técnica n. 49/2022/CGF/ANPD*, 2022, available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cgf_anpd_versao_publica.pdf).

¹⁶⁹ Gonçalves, J. B., ‘Quem vigia os vigilantes? O controle da atividade de inteligência no Brasil e o papel do Poder Legislativo’, *Revista de Informação Legislativa*, Brasília, a. 47, n. 187, 2010, available at: https://www12.senado.leg.br/ril/edicoes/47/187/ril_v47_n187_p125.pdf.

2.3 DATA SUBJECT RIGHTS

2.3.1 AVAILABLE RIGHTS AND THEIR SCOPE OF APPLICATION

The LGPD defines a minimum set of rights that should be respected by organisations processing personal data. Data subjects¹⁷⁰ have the right to (i) receive a confirmation that the data is being processed; (ii) access their data; (iii) rectify incomplete, inaccurate or outdated data; (iv) anonymisation, blocking or erasure of excessive data or within the scope of unlawful data processing; (v) data portability¹⁷¹, as long as it observes trade secrets; (vi) erasure of data processed under the consent of the data subject; (vii) obtain information about public and private entities with which the controller carried out shared use of data; (viii) obtain information about the possibility of not providing consent to a specific data processing and the consequences thereof; (ix) withdraw their consent; and (x) request the review of decisions based solely on automated means¹⁷².

In order to exercise their rights, the data subject or their representative must contact the data controller and this request should have no costs for the data subject. After the data subject's request, the controller must immediately answer the request. However, if this is not possible, the data controller must communicate that it does not process data from the data subject and indicate, whenever possible, the correct controller; or indicate the factual or legal reasons that prevent the immediate fulfilment of the request. From this point onwards, there are no specific rules on how long a controller may take to answer such requests, except in the case of the right to access, which demands that the controller provides a simplified version of the information immediately or a complete declaration in up to 15 days. For other requests, further guidelines from the ANPD are required. While the regulation is not published, controllers must respond to data subjects immediately (Article, paragraph 3º, LGPD).

Only in cases of omission by the controller or when the information provided raises questions about the legitimacy of the processing, has the data subject the right to bring the matter to the ANPD (Article 18 paragraph 1º; Article 55-J, V, LGPD) or consumer protection authorities (Article 18, paragraph 8º, LGPD), if this applies.

Prior to the LGPD, the CPC already contained provisions related to the protection of data sets and consumers' registration. It states that the consumer has the right to access their information, as well as the right to know where they were collected. The consumer also has the right to update any unprecise data, guaranteeing the data quality. All kinds of registers and data sets must be transparent, and the establishment of these sets must be notified to the consumer, when the processing was not requested by them. The CPC intended to address the issues related to a developing market in Brazil, the services of credit protection.

As explained by a national expert, there is a legal and ongoing debate on the extent to which the data subject rights apply to activities that are not in the scope of the LGPD. This is part of the discussion in the National Congress about a specific legislation to regulate these activities in more detail, as mentioned above. National experts also stated that data subjects will not be notified about the data processing in law enforcement activities, unless they become a part of the procedure (*e.g.*, provide a testimony, being prosecuted). In relation to data processing by public authorities more broadly, national experts also highlighted that it is still not clear if the right to erasure applies to their activities, since public authorities must comply with legal obligations related to keeping information in public files for historical purposes or even to be used as evidence in court.

¹⁷⁰ Article 18 and 20, LGPD.

¹⁷¹ The ANPD must develop further guidelines on the matter (Article 18, V, LGPD).

¹⁷² The LGPD does not provide for the right to have automated decisions reviewed by a human.

2.3.2 REDRESS MECHANISMS

2.3.2.1 RIGHT TO COMPENSATION AND LIABILITY

Article 42, LGPD, states that a controller or processor who causes material or non-material damages, be it individual or collective, while processing data in violation of LGPD is obliged to repair it. Data subjects can claim compensation collectively when the violation has affected multiple data subjects. Article 52, paragraph 7º, LGPD, also mentions the possibility that, in cases of data breaches or non-authorised access to data, this violation may be subject of direct conciliation between the controller and the data subject, and, if there is no agreement, penalties may also be applied by the ANPD. The ANPD guidelines also suggest that, in cases of data breaches or fraud, the police authority should be notified¹⁷³.

In relation to the liability of the controller or processor, it is important to mention that there is an ongoing doctrinal discussion on whether strict liability (no need to prove intent or fault) or a subject liability (proof of intent or fault is needed) applies to incidents involving personal data. Similar to what is seen in the GDPR, case-law will establish the liability system that should be applied. This doubt only applies to the situations outside the scope of the consumer protection code, since it explicitly adopts strict liability.

In a recent controversial decision, the STJ decided that, despite being an undesirable failure in the processing of personal information, a data breach cannot, by itself, cause non-material damages. Thus, in any claim for compensation, it is necessary for the data subject to prove the actual damage caused by the data breach¹⁷⁴.

As regards harm related to national security activities and law enforcement, the judiciary is responsible for dealing with both individual and collective claims. The Brazilian judiciary is competent to judge an action when the defendant, regardless of their nationality, is domiciled in Brazil; when the obligation has to be fulfilled in Brazil; or the basis for the procedure is a fact that occurred or an act performed in Brazil (Article 21, Civil Procedure Code)¹⁷⁵.

2.3.2.2 HABEAS DATA

Habeas Data is a fundamental right and constitutional remedy that guarantees the right of access to personal data held by public authorities or by public data sets. It is a summary, civil and free of charge procedure, that demands the participation of a lawyer in the procedure, and that can be used to: (i) guarantee the access of data being processed in registers or in data sets maintained by public authorities or public data sets; or (ii) rectify data, when this is not done within a confidential procedure (Article 5, LXXII and LXXVII, Constitution).

Any natural or legal person can be a holder of the legal claim, if the data is related to that person, regardless of their nationality. The only exception to this rule is the case of a surviving partner. The remedy can only be used after there is an omission or a refusal of the public authority (or the owner of the public data set) to access or correct the data¹⁷⁶. Thus, this redress mechanism requires that the data

¹⁷³ Autoridade Nacional de Proteção de Dados, *Petição de Titular*, 2022, available at: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados.

¹⁷⁴ Superior Tribunal de Justiça, *Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma*, 2023, available at: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/17032023-Titular-de-dados-vazados-deve-comprovar-dano-efetivo-ao-buscar-indenizacao--decide-Segunda-Turma.aspx>.

¹⁷⁵ Lei nº 13.105, de 16 de março de 2015, Código de Processo Civil, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm.

¹⁷⁶ The *Habeas Data* cannot be used if the administrative authority has not refused access to the information (Superior Tribunal de Justiça, Súmula 2, 1990, available at: <https://scon.stj.jus.br/SCON/SearchBRS?b=SUMU&livre=@NUM=2>).

subject is aware of the data processing, what may not always be the case for purposes of law enforcement, national security or intelligence activities.

2.4 FUTURE LEGISLATION

Work on the development of laws to fill the gaps left by the LGPD is already underway. As explained above, there are already discussions in the National Congress related to a specific law focused on data processing in public security and criminal prosecution activities.

Another national expert described that the legislative power in Brazil is active at the moment, and there are several proposed bills on different topics within the digital rights' realm. Bills regulating social media platforms and content moderation are also rising in Brazil. Currently, there are various cases focused on content moderation within the TSE and the STF. Recently, the Ministry of Justice and Public Safety stated that, alongside the Communications Secretariat (*Secretaria de Comunicação – SECOM* in the Portuguese acronym), a bill on the regulation of social media platforms is being developed¹⁷⁷.

Finally, taking into account the ANPD's regulatory agenda, several topics will start to be addressed in the near future. This comes after the development of the internal regulatory framework needed to guarantee the start of sanctioning activities by the authority.

2.5 OVERVIEW OF RELEVANT LEGISLATION

Public authority activity	Laws applied	Oversight	Redress mechanisms
Intelligence purposes	Law n. 9883/99 Constitution	Legislative bodies	N/A
Law enforcement purposes	Telephone Interception Law Criminal Procedures Code	Judiciary	Judiciary
General rules of data access	LGPD Constitution Habeas Data Law Decree n. 10.046/19	ANPD Judiciary Constitutional control	ANPD Judiciary

¹⁷⁷ Índio do Brasil, C., 'Dino: governo prepara PL para regulamentação das redes sociais', *Agência Brasil*, 13 March 2023, available at: https://agenciabrasil.ebc.com.br/politica/noticia/2023-03/dino-governo-prepara-pl-para-regulamentacao-das-redes-sociais?utm_source=meio&utm_medium=email.

3 CONCLUSION

This study has assessed the relevant legal frameworks and practices around governmental access for Brazil. The paragraphs below summarise the main findings of the report.

Brazil has a fairly new legal data protection framework. Recent years' achievements include the approval of a general law, the creation of the ANPD, the enshrinement of data protection as a fundamental right in the Brazilian Constitution, ascending to the Budapest Convention, and the development of a data protection culture through jurisprudence, doctrine and guidance documents. The LGPD presents a structured system to guarantee the rights to privacy and to the protection of personal data, with a very similar approach to the GDPR.

While the LGPD presents a solid and extensive data protection framework, comprehensive rules on national security, public security, national defence, and criminal procedure need to be developed. Criminal procedures do have to comply with a fragmented, but robust, legal framework. Consequently, the majority of surveillance measures are overseen and controlled by judicial authorities (e.g., the need for a judicial order for the interception of telecommunications or adjudicating a lawsuit). Data processing for national security and national defence, on the other hand, has less rigid legal limits, with the judiciary and the legislature as their main oversight bodies. As seen, the LGPD determines that its principles and data subject rights must be included in the specific legislation to be developed, in addition to providing for proportional and strictly necessary measures to serve the public interest, subject to due process of law. National experts are of the opinion that these provisions already apply to activities outside of the scope of the LGPD. However, a specific law providing details of the application of the right to data protection in these cases is crucial to protect data subjects and provide legal certainty. Furthermore, it is still to be seen how the ANPD will deal with these exceptions, in view of its specific competence in these cases to issue technical opinions and recommendations, as well as to request reports on the impact on the protection of personal data.

ANNEX 1 – QUESTIONNAIRE

Brazil

General questions

1. How are necessity and proportionality evaluated when public authorities have access to personal data? Are there any legal obligations on this matter (e.g., need for publishing the assessment)? In recent years, there has been news regarding the monitoring of public employees by Brazilian public authorities. Has this issue been addressed? How?
2. Are there any cases/situations where a judicial decision is not needed for a government body to have access to personal data for investigation purposes or national security?
3. According to the Constitution, fundamental rights are guaranteed to foreigners living in Brazil. Do foreigners, including EU citizens, who live outside of Brazil also have their rights guaranteed?
4. Are there legally binding safeguards for the processing of personal data for intelligence and law enforcement purposes?
5. Brazil has been working on different initiatives to guarantee the digitalisation of identities and develop smart cities. Are safeguards being discussed in these projects? Who is participating in these discussions?
6. Are there any proposed bills or paradigmatic court decisions regarding the use of malware for lawful surveillance practices?
7. Some sensitive topics (e.g., government access for intelligence purposes) depend on presidential acts. Does this model bring a lot of legal uncertainty to the system? What has been the main understanding regarding the exceptions of data usage for intelligence purposes?
8. Are there any bills to address cybersecurity minimum grounds that should be followed in the country? Did the adoption of the Budapest Convention make any significant changes in the Brazilian regulatory framework? Does this new regulatory framework avoid the usage of unsafe surveillance technologies by the government?
9. How is personal data protected in the processing for criminal persecution, national defence and security or public safety, considering the existing legal gap (e.g., the fact that the Brazilian Data Protection law does not apply to these cases)?
10. What are the existing rules on data sharing from one Brazilian public authority to another (onward sharing)? How do data subject rights apply in these situations?
11. What are the existing rules regarding data transfers from Brazil to other (third) countries, especially when the personal data was collected or accessed by a Brazilian public authority?

Data subject rights

12. Considering the secrecy of the police investigation, how and when is the data subject informed about the collection of his/her personal data for crime investigation or national

security purposes?

13. What oversight is there for the access of personal data by regulatory agencies (*agências reguladoras*, i.e., ANATEL)? Are there any redress mechanisms for the data subject to guarantee her/his data subject rights?

Case law

14. Were the last decisions of the Superior Court of Justice and Supreme Court of Justice enough to guarantee the respect of data protection principles in activities out of the scope of the Brazilian Data Protection Law (e.g., public, and national security)?
15. How are the regulatory framework and national practices adapting to the recent court decisions regarding the use of facial technology in public spaces?

Remedies and redress mechanisms

16. The Brazilian Data Protection Supervisory Authority just turned independent. How do you evaluate the work of the SA until now? Did the administrative change make any significant difference in its work?
17. Is it possible to consider that the Brazilian SA has focused more on normative work following its regulatory agenda than in evaluating specific cases? What is your opinion on this choice?

ANNEX 2 – SOURCES OF INFORMATION

General Part

Case law

CJEU

- Judgment of the Court (Grand Chamber) of 20 September 2022, C-339/20 VD and C-397/20 SR, ECLI:EU:C:2022:703.
- Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D v The Commissioner of the Garda Síochána, and Others*, C-140/20, ECLI:EU:C:2022:258.
- Judgment of the Court (Tenth Chamber) of 21 October 2021, *the Spetsializiran nakazatelen sad*, C-350/21, ECLI:EU:C:2021:874.
- Judgment of the Court (Eighth Chamber) of 2 September 2021, *Telekom Deutschland GmbH v Bundesrepublik Deutschland*, C-794/19.
- Judgment of the Court (Grand Chamber) of 22 June 2021, *Ordre des barreaux francophones et germanophone and others*, C-512/18, ECLI:EU:C:2021:505.
- Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, ECLI:EU:C:2021:152.
- Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.
- Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18, ECLI:EU:C:2020:791.
- Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, ECLI:EU:C:2020:559.
- Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.
- Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14 ECLI:EU:C:2015:650.
- Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.
- Judgment of the Court (Fourth Chamber) of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670.
- Judgment of the Court (Grand Chamber), 26 February 2013, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2013:107.
- Judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727.
- Judgment of the Court of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596.
- Judgment of the Court (Grand Chamber) of 20 September 2022, *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH.SpaceNet*, C-793/19, ECLI:EU:C:2022:702.

ECtHR

- Judgement of 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013.
- Judgement of 4 December 2015, *Zakharov v. Russia*, no. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306.
- Judgement of 18 May 2010, *Kennedy v. the United Kingdom*, no. 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905.
- Judgement of 2 December 2008, *K.U. v. Finland*, no. 2872/02, ECLI:CE:ECHR:2008:1202JUD000287202.
- Judgement of 29 June 2006, *Weber and Saravia*, no. 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400.

Judgement of 4 March 2004, <i>M.C. v. Bulgaria</i> , no. 39272/98, ECLI:CE:ECHR:2003:1204JUD003927298.
Judgement of 4 May 2000, <i>Rotaru v. Romania</i> , no. 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195.
Judgement of 16 February 2000, <i>Amann v. Switzerland</i> , no. 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895.
Judgement of 28 October 1998, <i>Osman v. United Kingdom</i> , no. 23452/94, ECLI:CE:ECHR:1998:1028JUD002345294.
Judgement of 24 April 1990, <i>Huvig v. France</i> , no. 11105/84.
Judgement of 26 March 1987, <i>Leanderv. Sweden</i> , no. 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881.
Judgement of 2 August 1984, <i>Malone v. the UK</i> , no. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179.
Judgement of 26 April 1979, <i>The Sunday Times v. the UK</i> , no. 6538/74, ECLI:CE:ECHR:1979:0426JUD000653874.

Opinions

Opinion of the Court (Grand Chamber) of 26 July 2017, Opinion 1/15 on the EU-Canada PNR Agreement, ECLI:EU:C:2017:592.

Other sources

- European Data Protection Board (2023), *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.
- European Data Protection Board (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*.
- European Data Protection Board (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*.
- European Data Protection Supervisor (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*.
- European Data Protection Supervisor (2021), *Case Law Digest: Transfers of personal data to third countries*.
- European Data Protection Supervisor (2019), *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*.
- European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018.
- Gerards, J., ‘How to improve the necessity test of the European Court of Human Rights’, *International Journal of Constitutional Law*, Vol. 11, No 2, April 2013, pp. 466–490.
- Lenaerts, K., ‘Limits on Limitations: The Essence of Fundamental Rights in the EU’, *German Law Journal*, Vol. 20, pp. 779-793, Cambridge University Press, 2019.
- Brkan, M., ‘The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU’s constitutional reasoning’, *German Law Journal*, Vol. 20, pp. 864-883, Cambridge University Press, 2019.
- Tridimas, T., Gentile, G., ‘The essence of Rights: An Unreliable Boundary?’, *German Law Journal*, Vol. 20, pp. 794–816, Cambridge University Press, 2019.
- Tracol, X., ‘Ministerio fiscal: Access of public authorities to personal data retained by providers of electronic communications services’, *European Data Protection Law Review*, Vol. 5, No 1, pp. 127-135.

Brazil

Case law

Superior Tribunal de Justiça, REsp 1355432-SP, 2014, available at:
https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201202488103.

Superior Tribunal de Justiça, RHC 75800/PR, 2016, available at:
<https://processo.stj.jus.br/webstj/Processo/justica/jurisprudencia.asp?valor=201602394838>.

Superior Tribunal de Justiça, Súmula 2, 1990, available at:
<https://scon.stj.jus.br/SCON/SearchBRS?b=SUMU&livre=@NUM=2>.

Supremo Tribunal Federal, ADC 51, 2023, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>.

Supremo Tribunal Federal, ADI 5527, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>.

Supremo Tribunal Federal, ADI 6387, 2020, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>.

Supremo Tribunal Federal, ADI 6529, 2021, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837>.

Supremo Tribunal Federal, ADI 6649, 2022, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238>.

Supremo Tribunal Federal, ADPF 403, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500>.

Supremo Tribunal Federal, ADPF 695/DF, 2022, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693>.

Supremo Tribunal Federal, ARE 1316369/DF, 2022, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=6129951>.

Supremo Tribunal Federal, HC 96986/MG, 2012, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=2649995>.

Supremo Tribunal Federal, HC 108147/PR, 2012, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401>.

Supremo Tribunal Federal, HC 128102/SP, 2015, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4770762>.

Supremo Tribunal Federal, HC 133148/ES, 2017, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4932933>.

Supremo Tribunal Federal, HC 129678/SP, 2018, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4820467>.

Supremo Tribunal Federal, MS 25940, 2018, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=2376827>.

Supremo Tribunal Federal, MS 34751/CE, 2018, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5172309>.

Supremo Tribunal Federal, RE 587970/SP, 2017, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=2621386>.

Supremo Tribunal Federal, RE 1018911/RR, 2021, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5115280>.

Supremo Tribunal Federal, RHC 132062/RS, 2016, available at:
<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4903009>.

Tribunal de Contas da União, Processo n. 014.760/2021-5, 2022.

Legislation

Constituição da República Federativa do Brasil de 1988, available at:
https://www.planalto.gov.br/ccivil_03/constituciona/constituicao.htm.

Decreto-Lei nº 2.848, de 7 de Dezembro de 1940, Código Penal, available at:
http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

Decreto-Lei nº 3.689, de 3 de Outubro de 1941, Código de Processo Penal, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

Decreto-Lei nº 4.657, de 4 de setembro de 1942, Lei de Introdução às Normas do Direito Brasileiro, 1942, available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm.

Decreto Legislativo nº 37 de 16 de Dezembro de 2021, Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, available at: <https://legis.senado.leg.br/norma/35289207>.

Decreto nº 4.376, de 13 de Setembro de 2022, Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999, e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/decreto/2002/d4376.htm.

Decreto nº 9.637, de 26 de Dezembro de 2018, Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional, available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm#:~:text=DECRETO%20N%C2%BA%209.637%2C%20DE%2026,regulamenta%20o%20disposto%20no%20art.

Decreto nº 10.222, de 5 de fevereiro de 2020, Aprova a Estratégia Nacional de Segurança Cibernética, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

Decreto nº 11.348, de 1º de Janeiro de 2023, Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão e funções de confiança, available at: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm.

Lei Complementar nº 75, de 20 de maio de 1993, Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União, available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp75.htm.

Lei nº 8.069, de 13 de Julho de 1990, Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

Lei nº 8.078, de 11 de Setembro de 1990, Dispõe sobre a proteção do consumidor e dá outras providências, available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

Lei nº 9.296, de 24 de Julho de 1996, Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, available at: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

Lei nº 9.784, de 29 de Janeiro de 1999, Regula o processo administrativo no âmbito da Administração Pública Federal, available at: http://www.planalto.gov.br/ccivil_03/leis/l9784.htm#:~:text=LEI%20N%C2%BA%209.784%20%2C%20DE%2029%20DE%20JANEIRO%20DE%201999.&text=Regula%20o%20processo%20administrativo%20no%20C3%A2mbito%20da%20Administra%C3%A7%C3%A3o%20P%C3%A7%C3%BAblica%20Federal.

Lei nº 9.883, de 7 de Dezembro de 1999, Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências, available at: https://www.planalto.gov.br/ccivil_03/leis/l9883.htm.

Lei nº 9.986, de 18 de Julho de 2000, Dispõe sobre a gestão de recursos humanos das Agências Reguladoras e dá outras providências, available at: http://www.planalto.gov.br/ccivil_03/leis/l9986.htm.

Lei nº 10.406, de 10 de Janeiro de 2002, Institui o Código Civil, available at: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm.

Lei nº 12.414, de 9 de Junho de 2011, Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

Lei nº 12.527, de 18 de Novembro de 2011, Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e

- dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências*, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.
- Lei nº 12.965, de 23 de Abril de 2014, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
- Lei nº 13.105, de 16 de março de 2015, Código de Processo Civil*, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm.
- Lei nº 13.445, de 24 de Maio de 2017, Institui a Lei de Migração*, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o.&text=Art.,pol%C3%ADticas%20p%C3%ABlicas%20para%20o%20emigrante.
- Lei nº 13.709, de 14 de Agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD)*, available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
- Lei nº 13.853, de 9 de Julho de 2019, Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm.
- Lei nº 14.460, de 25 de Outubro de 2022, Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019*, available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14460.htm.

Other sources

- Amnesty International (2023), *Amnesty International Report 2022/23: The State of the World's Human Rights*, available at: <https://www.amnesty.org/en/location/americas/south-america/brazil/report-brazil/>.
- Amnesty International, *Police Violence*, available at: <https://www.amnesty.org/en/what-we-do/police-brutality/>.

- Associação Data Privacy Brasil de Pesquisa, *Intervenção como amicus curiae - Ação Direta de Inconstitucionalidade nº 6.649, https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755538665&prcID=60792 38.*
- Autoridade Nacional de Proteção de Dados - ANPD, available at: <https://www.gov.br/anpd/pt-br>.
- Autoridade Nacional de Proteção de Dados, *ANPD divulga balanço de acompanhamento e execução da Agenda Regulatória 2021/2022 referente ao 2º semestre de 2022*, 16 January 2023, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-balanco-semestral-de-acompanhamento-e-execucao-da-agenda-regulatoria-2021-2022>.
- Autoridade Nacional de Proteção de Dados, *ANPD e Ministério da Justiça e Segurança Pública editam portaria conjunta*, 13 February 2023, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-ministerio-da-justica-e-seguranca-publica-editam-portaria-conjunta>.
- Autoridade Nacional de Proteção de Dados, *ANPD manifesta-se sobre divulgação de microdados do Enem e Censo Escolar pelo INEP*, 17 Mai 2022, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-manifesta-se-sobre-divulgacao-de-microdados-do-enem-e-censo-escolar-pelo-inep>.
- Autoridade Nacional de Proteção de Dados, *ANPD publica Agenda de Avaliação de Resultados Regulatórios*, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-de-avaliacao-de-resultados-regulatórios>.
- Autoridade Nacional de Proteção de Dados (2021), *Nota Técnica n. 02/2021/CGTP/ANPD*, available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NotaTecnicaANPDWhatsapp_ocr.pdf.

- Autoridade Nacional de Proteção de Dados (2021), *Nota Técnica n. 19/2021/CGF/ANPD*, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTcnica19.2021.CGF.ANPD.pdf>.
- Autoridade Nacional de Proteção de Dados (2022), *Nota Técnica n. 49/2022/CGF/ANPD*, available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf.
- Autoridade Nacional de Proteção de Dados (2022), *Petição de Titular*, available at: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados.
- Autoridade Nacional de Proteção de Dados, *Portaria ANPD n. 35, de 4 de novembro de 2022, Agenda Regulatória para o biênio 2023-2024*, available at: <https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885>.
- Autoridade Nacional de Proteção de Dados, *Resolução CD/ANPD n. 4, de 24 de fevereiro de 2023, Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas*, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucao4CDANPD24.02.2023.pdf>.
- Autoridade Nacional de Proteção de Dados, *Resolução CD/ANPD n. 5, de 13 de março de 2023, Agenda de Avaliação de Resultado Regulatório para o período 2023-2026*, available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-de-avaliacao-de-resultados-regulatorios/RESOLUON5ARR.pdf>.
- Autoridade Nacional de Proteção de Dados (2022), *Tratamento de Dados Pessoais pelo Poder Público*, available at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>.
- Belli, L. et al (2023), *Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil digitalmente soberano*, available at: <https://cyberbrics.info/ciberseguranca-uma-visao-sistematica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/>.
- Bioni, B. R., Silva, P. G. F., Martins, P. B., ‘Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso’, *Cadernos técnicos da CGU: coletânea de artigos da pós-graduação em ouvidoria pública*, 2022, pp. 8–19.
- Câmara dos Deputados do Brasil, *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*, 2019, available at: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf>.
- Câmara dos Deputados, PL 1515/2022, available at: <https://www.camara.leg.br/propostas-legislativas/2326300>.
- Campos, A. C., ‘Drones são adotados por 63% das forças de segurança no Brasil’, *Agência Brasil*, 29 March 2023, available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2023-03/drones-sao-adoptados-por-63-das-forcas-de-seguranca-no-brasil>.
- Cano, I., ‘Public Security Policies in Brazil: Attempts to Modernize and Democratize versus the War on Crime’, *Sur*, Number 5, Year 3 , 2006, available at: <https://sur.conectas.org/en/public-security-polices-brazil/>.

- Conselho da Justiça Federal, *IX Jornada de Direito Civil, Enunciado 678*, 2022, available at: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf/view>.
- Conselho Nacional dos Procuradores-Gerais, *Manual Nacional do Controle Externo da Atividade Policial*, 2009, available at: http://www.mppsp.mp.br/portal/page/portal/cao_crime/CAOCri_ControleExtAtivPol/Manual%20Nacional%20do%20Controle%20Externo%20da%20Atividade%20Policial.pdf.

Controladoria-Geral da União, *CGU e ANPD firmam parceria para cooperação entre os órgãos*, 17 February 2023, available at: <https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/02/cgu-e-anpd-firmam-parceria-para-cooperacao-entre-os-orgaos>.

Council of Europe, *Brazil and the Data protection Commission of Gabon to join the Committee of Convention 108 as observers*, 12 October 2018, available at: <https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers->.

Council of Europe, *Brazil accedes to the Convention on Cybercrime and six States sign the new Protocol on e-evidence*, 30 November, 2022, available at: <https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence>.



Fiquem Sabendo, INSPER, FGV, *Impactos da LGPD nos pedidos de LAI ao governo federal*, 2022, available: at https://drive.google.com/file/d/1LfYUOjNVyxC1LAL3U_fGwWSCNL7t16ap/view.

Gonçalves, J. B., ‘Quem vigia os vigilantes? O controle da atividade de inteligencia no Brasil e o papel do Poder Legislativo’, *Revista de Informação Legislativa*, Brasília, Vol 47, No 187, 2010, available at: https://www12.senado.leg.br/ril/edicoes/47/187/ril_v47_n187_p125.pdf.

Grossman, L. O., ‘ANPD recebeu 120 indicações para Conselho Nacional de Proteção de Dados’, *Convergência Digital*, 26 March 2021, available at: <https://www.convergenciadigital.com.br/Seguranca/ANPD-recebeu-120-indicacoes-para-Conselho-Nacional-de-Protecao-de-Dados-56510.html?UserActiveTemplate=site>.

Human Rights Council, A/HRC/27/3, *The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights*, available at https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.ohchr.org%2Fsites%2Fdefault%2Ffiles%2FDocuments%2FIssues%2FDigitalAge%2FA-HRC-27-37_en.doc%23%3A~%3Atext%3DIn%2520its%2520resolution%252068%252F167%2Ccommunications%2520and%2520the%2520collection%2520of&wdOrigin=BROWSELINK.

Hurel, L. M., ‘Cybersecurity in Brazil: An analysis of the National Strategy’, *Igarapé Institute*, 2021, available at: https://igarape.org.br/wp-content/uploads/2021/04/SP-54_Cybersecurity-in-Brazil.pdf.

Hurel, L. M., Lobato, L. C., ‘A Strategy for Cybersecurity Governance in Brazil’, *Igarapé Institute*, 2019, available at: <https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf>.

Índio do Brasil, C., ‘Dino: governo prepara PL para regulamentação das redes sociais’, *Agência Brasil*, 13 March 2023, available at: https://agenciabrasil.ebc.com.br/politica/noticia/2023-03/dino-governo-prepara-pl-para-regulamentacao-das-redes-sociais?utm_source=meio&utm_medium=email.

Instituto Igarapé, *Documents - Portal Brasileiro da Cibersegurança*, available at: <https://ciberseguranca.igarape.org.br/en/category/documents/>.

Instituto Igarapé, *Implementação de Tecnologias de Vigilância no Brasil e na América Latina*, 2022, available at: <https://igarape.org.br/wp-content/uploads/2022/12/Implementacao-de-tecnologias-de-vigilancia-no-brasil-e-na-america-latina.pdf>.

Instituto Igarapé, *Reconhecimento Facial no Brasil*, available at <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>.

Instituto Igarapé, ‘The Brazilian Cybersecurity Ecosystem’, *Portal Brasileiro de Cibersegurança*, available at: <https://ciberseguranca.igarape.org.br/en/ecosystem/>.

International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI)*, 2018, https://www.itu.int/dms_pub/itu-d/obp/str/D-STR-GCI.01-2018-PDF-E.pdf.

International Telecommunication Union (ITU), *Global Cybersecurity Index (CGI)*, 2020, available at available at: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>.

Laboratório de Pesquisa em Políticas Públicas e Internet (LAPIN), *Nota Técnica - Derrubada dos Decretos 10.046/2019 e 10.047/2019 - Compartilhamento de dados no âmbito da administração*

- pública federal, <https://lapin.org.br/wp-content/uploads/2020/08/NT.-2-Derrubada-dos-Decretos-10.0462019-e-10.0472019.-LAPIN.pdf>.
- Maia, F., ‘STF: MLAT é constitucional, mas acordo não é a única forma de obtenção e prova’, *Jota*, 23 February 2023, available at: <https://www.jota.info/stf/do-supremo/stf-mlat-e-constitucional-mas-acordo-nao-e-a-unica-forma-de-obtencao-de-prova-23022023>.
- Mendes, L. S., ‘A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis’, *Caderno Especial LGPD*, São Paulo, RT, November 2019, pp. 35-56.
- Mendes, L. S., ‘Democracia, poder informacional e vigilância’, *OGlobo*, 13 August 2022, available at: <https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml>.
- Mendes, L. M., Gasiola, G. G., ‘Inconstitucionalidade do Decreto 10.046: limites do compartilhamento de dados’, *Conjur*, 14 September 2022, available at: <https://www.conjur.com.br/2022-set-14/schertel-gasiola-compartilhamento-dados-setor-publico>.
- Ministério da Defesa, *Estratégia Nacional de Defesa*, 2008, available at: <http://livroaberto.ibict.br/bitstream/1/605/2/Estrategia-Nacional-de-Defesa.pdf>.
- Ministério da Justiça e Segurança Pública, *Governo lança debate público sobre regulamentação de lei e anteprojeto*, 28 January 2015, available at: <https://www.gov.br/mj/pt-br/assuntos/noticias/governo-lanca-debate-publico-sobre-regulamentacao-de-lei-e-anteprojeto>.
- Nunes, P., Silva, M. R., Oliveira, S. R. de, ‘A Rio of cameras with selective eyes: the use of facial recognition by the Rio de Janeiro state police’, *O Panóptico*, 2022, available at: https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPTI_riodecameras_mar22_0404b_english.pdf.
- OECD, *OECD takes first step in accession discussions with Argentina, Brazil, Bulgaria, Croatia, Peru and Romania*, 25 January 2022, available at: <https://www.oecd.org/newsroom/oecd-takes-first-step-in-accession-discussions-with-argentina-brazil-bulgaria-croatia-peru-and-romania.htm>.
- Parentoni, L., Lima, H. ‘Proteção de Dados Pessoais no Brasil: Antinomias Internas e Aspectos Internacionais’, *Direito & Internet: Sistema de Proteção de Dados Pessoais*, 2019, pp. 483-512.
- Pereira, A. B. C., Cabral, S., Reis, P. R. da C., ‘Accountability interna em forças policiais: explorando os fatores associados ao desempenho de uma corregedoria de polícia militar’, *Organizações & Sociedade*, 27(92), 2020, available at: <https://doi.org/10.1590/1984-9270922>.
- Petrocilo, C., Lacerda, L., Seto, G., ‘Prefeitura revê, mas não desiste de programa de reconhecimento facial em SP’, *Folha de São Paulo*, 2 December 2022, available at: <https://www1.folha.uol.com.br/cotidiano/2022/12/suspensao-apos-criticas-projeto-de-reconhecimento-facial-sera-mantido-diz-nunes.shtml>.
- Presidência da República, *Estratégia de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética da Administração Pública Federal (APF)*, 2013, available at: <https://www.gov.br/gsi/pt-br/assuntos/noticias/2015/estrategia-de-seguranca-da-informacao-e-comunicacoes-sic-e-de-seguranca-cibernetica-da-administracao-publica-federal-apf>.
- Presidência da República, *Livro Verde Segurança Cibernética no Brasil*, 2010, available at https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf.

Rebelo, A., ‘O mecenás’, *The Intercept*, 5 April 2023, available at <https://www.intercept.com.br/2023/04/05/delegado-waldir-torrou-r-30-milhoes-em-reconhecimento-facial-para-cidades-que-sequer-tem-saneamento-em-goias/>.

Santos, B. M., ‘Convenção de Budapeste Sobre o Cibercrime na América Latina: uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México’, *Derechos Digitales*, 2022, available at <https://www.derechosdigitales.org/wp-content/uploads/PT-Ciberdelincuencia-2022.pdf>.

- Souza, C. A., Viola, M., Lemos, R., ‘Brazil’s Internet Bill of Rights: A Closer Look’, *Instituto de Tecnologia e Sociedade*, 2018, available at https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf
- Souza, N., ‘ANPD mira em punições para garantir cumprimento da lei de dados’, *Jota*, 6 February 2023, available at <https://www.jota.info/coberturas-especiais/protecao-de-dados/anpd-mira-em-punicoes-para-garantir-cumprimento-da-lei-de-dados-06022023>,
- Superior Tribunal de Justiça, *Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma*, 2023, available at <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/17032023-Titular-de-dados-vazados-deve-comprovar-dano-efetivo-ao-buscar-indenizacao--decide-Segunda-Turma.aspx>.
- Supremo Tribunal Federal, *STF confirma limitações ao compartilhamento de dados do Sisbin*, 15 October 2021, available at <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=474835&ori=1>.
- Le Temps, *Une opération policière dans une favela de Rio fait au moins 22 morts*, 24 May 2022, available at <https://www.letemps.ch/monde/ameriques/une-operation-policiere-une-favela-rio-22-mort>.
- Tire meu Rosto da Sua Mira (2022), *Open Letter to Ban the Use of Digital Facial Recognition Technologies in public Security*, available at <https://tiremeurostodasuamira.org.br/en/open-letter/>.
- United Nations, *Brazil: UN experts decry acts of racialised police brutality*, 6 July 2022, available at: <https://www.ohchr.org/en/press-releases/2022/07/brazil-un-experts-decrys-racialised-police-brutality>.
- Vassallo, L., Kattah, E., Medeiros, D., ‘Governo Lula vai rever cooperação do MPF com outros países; medica foi central na Lava Jato’, *Estadão*, available at <https://www.estadao.com.br/politica/governo-lula-vai-rever-cooperacao-do-mpf-com-outros-paises-medida-foi-central-na-lava-jato/>.
- Vlois, R., ‘Tecnoautoritarismo e o bloqueio de provedores por descumprimento de ordens judiciais no Brasil’, *Nexo Jornal*, 26 January 2023, available at <https://pp.nexojornal.com.br/opiniao/2023/Tecnoautoritarismo-e-o-blockio-de-provedores-por-descumprimento-de-ordens-judiciais-no-Brasil>.
- Wimmer, M., ‘O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público’, *Tratado de Proteção de Dados Pessoais*, 1. ed., Rio de Janeiro, Forense, 2021. pp. 271–288.

ANNEX 3 – ACRONYMS AND ABBREVIATIONS

General

Acronyms and Abbreviations	Meaning
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Convention 108+	Convention 108+ on protection of individuals with regard to the Processing of Personal Data
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
EU-Charter	Charter of Fundamental Rights of the European Union
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
HRC	United Nations Human Rights Council
HRW	Human Rights Watch
ICCPR	International Covenant on Civil and Political Rights
OECD	Organisation for Economic Co-operation and Development
SA(s)	Supervisory authority(-ies)
UDHR	Universal Declaration of Human Rights
UN	United Nations

Brazil

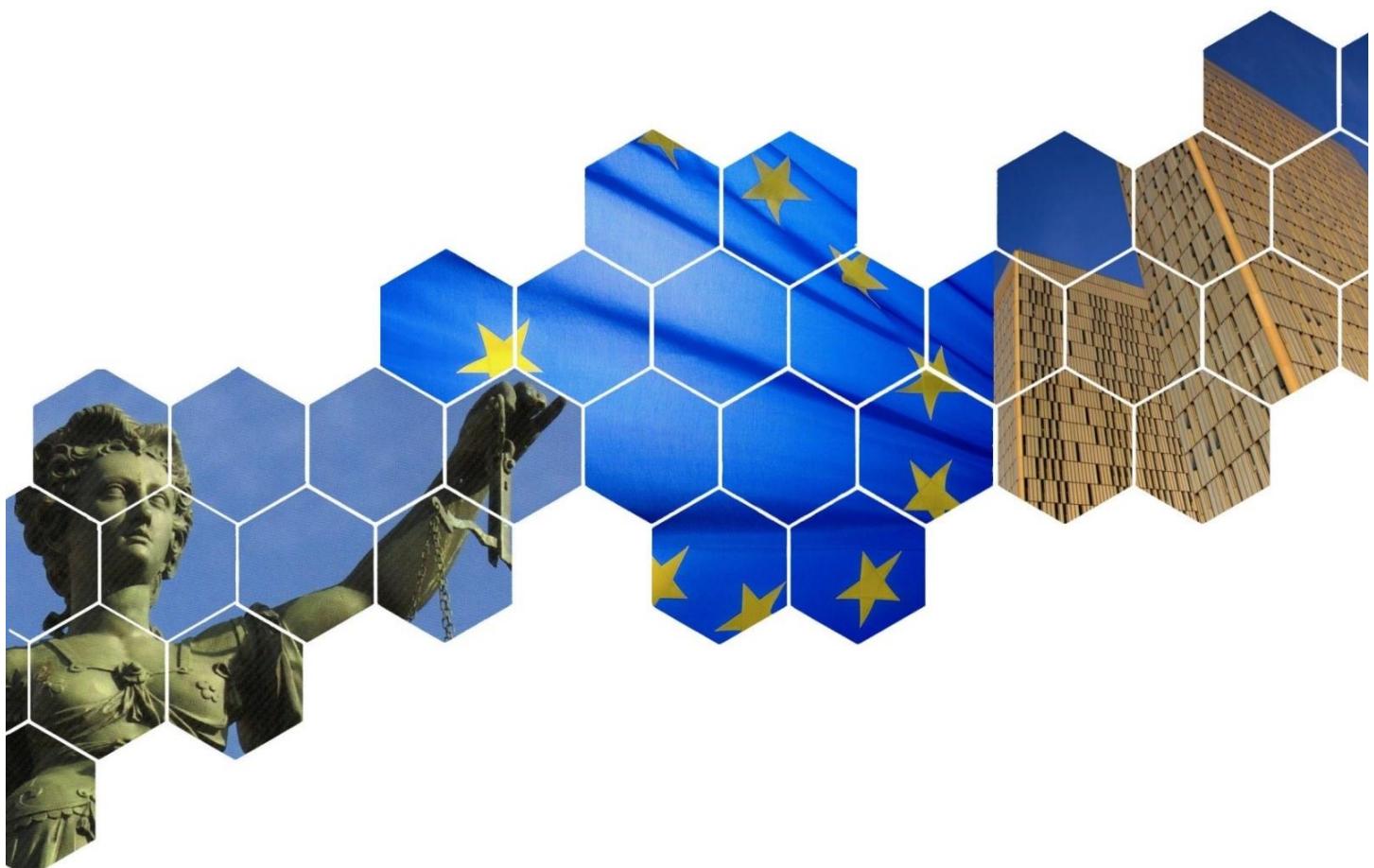
Acronyms and Abbreviations	Meaning
ABIN	Brazilian Agency of Intelligence (<i>Agência Brasileira de Inteligência</i>)
ANPD	Brazilian Data Protection Supervisory Authority (<i>Autoridade Nacional de Proteção de Dados</i>)
ARR	Regulatory Results Assessment (<i>Avaliação de Resultados Regulatórios</i>)
CADE	Administrative Council of Economic Defense – Brazilian Antitrust Body (<i>Conselho Administrativo de Defesa Econômica</i>)
CCAI	Joint Commission for Control of Intelligence Activities of the National Congress (<i>Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional</i>)
CGU	Office of the Comptroller General (<i>Controladoria Geral da União</i>)
CPI	Parliamentary Investigation Committee (<i>Comissão Parlamentar de Inquérito</i>)
CDC	Consumer Protection Code (<i>Código de Defesa do Consumidor</i>)
CNPD	National Council for Data Protection and Privacy (<i>Conselho Nacional de Proteção de Dados Pessoais e da Privacidade</i>)
DENATRAN	National Traffic Department (<i>Departamento Nacional de Trânsito</i>)

DRCI	Department of Asset Recovery and International Cooperation (Departamento de Recuperação de Ativos e Cooperação Internacional)
ENEM	National Examination of Secondary Education (Exame Nacional do Ensino Médio)
INEP	National Institute of Educational Studies and Research Anísio Teixeira (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira)
LAI	Access to Public Information Law (Lei de Acesso à Informação)
LGPD	Brazilian Data Protection Law (Lei Geral de Proteção de Dados)
LINDB	Law of Introduction to the Rules of Brazilian Law (Lei de Introdução às Normas do Direito Brasileiro)
MCI	Civil Rights Framework for the Internet in Brazil (Marco Civil da Internet)
MLAT	Mutual Legal Assistance Treaty
MPF	Federal Public Prosecutor's Office (Ministério Públíco Federal)
OECD	Organisation for Economic Co-operation and Development
SBI	Brazilian Intelligence System (Sistema Brasileiro de Inteligência)
SECOM	Communications Secretariat (Secretaria de Comunicação)
SENACON	National Consumer Secretariat (Secretaria Nacional do Consumidor)
STF	Supreme Federal Court (Supremo Tribunal Federal)
STJ	Superior Court of Justice (Superior Tribunal de Justiça)
TCU	Federal Court of Accounts (Tribunal de Contas da União)
TSE	Superior Electoral Court (Tribunal Superior Eleitoral)

Government access to data in third countries II

Final Report

Specific Contract No. 2022-0716
Implementing the Framework Contract EDPS/2019/02



KU LEUVEN

April 2023

This study has been prepared by Milieu under Contract No 2022-0716 (EDPS/2019/02) for the benefit of the EDPB.



The study has been carried out by researchers from CiTiP, KU Leuven, with the support of Milieu Consulting SRL. The authors of the study are Dr Laura Drechsler, Abdullah Elbi, Elora Fernandes, Eyup Kun, Isabela Maria Rosal, Bilgesu Sumer, and Dr Sofie Royer from CiTiP, KU Leuven.

The information and views set out in this study are those of the author(s) and do not reflect the official opinion of the EDPB. The EDPB does not guarantee the accuracy of the data included in this study. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for the use which may be made of the information contained therein.

This study does not bind the EDPB and its members in their assessment of individual data transfers. This study is not an “adequacy finding” for which the European Commission alone is competent under Regulation (EU) 2016/679 (GDPR) and Directive (EU) 2016/680 (LED).

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be; web address: www.milieu.be.

Table of contents

EXECUTIVE SUMMARY.....	4
1 INTRODUCTION	5
1.1 Objectives and scope of the study	5
1.2 Legal background	5
1.2.1 Data transfers in the GDPR	6
1.2.2 Interferences with the fundamental rights under the EU-Charter ...	6
1.2.3 Legality of governmental access	7
1.2.4 Objectives of general interest or protection of rights and freedoms of others	8
1.2.5 Necessity and proportionality	9
1.2.6 Respect the essence of the right.....	10
1.3 Study methodology	11
1.4 Structure of this report	12
2 IN-DEPTH ANALYSIS OF THIRD COUNTRIES.....	13
2.1 Mexico	14
2.1.1 Rule of law, respect for human rights and fundamental freedoms	14
2.1.2 Governmental access to personal data.....	23
2.1.3 Data subject rights	28
2.1.4 Overview of relevant legislation	31
2.2 Türkiye	32
2.2.1 Rule of law, respect for human rights and fundamental freedoms	32
2.2.2 Governmental access to personal data.....	37
2.2.3 Data subject rights	48
2.2.4 Overview of relevant legislation	50
3 CONCLUSION.....	52
ANNEX 1 – QUESTIONNAIRES	54
ANNEX 2 – SOURCES OF INFORMATION.....	58
ANNEX 3 – ACRONYMS AND ABBREVIATIONS.....	65

EXECUTIVE SUMMARY

This report provides information on the legislation and practices in Mexico, and Türkiye for the situation where personal data are accessed by governmental authorities for reasons of national security or law enforcement (governmental access). This study was based on a literature review via desk research (books, journal articles, databases and other online sources), also including reports of international organisations on the country in question. The legal analysis based on the literature review and the relevant legal documents was complemented by a round of interviews with carefully selected experts with the goal of gaining insights into the practice of the analysed laws. The main findings of this approach for each country are outlined in the following paragraphs.

Mexico has a multi-layered data protection framework. Constitutionally, not only the right to data protection is guaranteed to every person, regardless of nationality, but also the data subjects' rights of access, rectification, cancellation, and opposition. Any data processing carried out by private parties in Mexico must comply with the Data Protection Law for Private Parties (LFPSSP), which the National Institute for Transparency, Access to Information, and Data Protection (INAI) oversees. For the public sector, Mexico adopted the Data Protection Law for Public Parties (LGPDSSO) in 2015. This general law establishes the main rules for data protection in the public sector while dividing competences between the 33 different federal entities in Mexico. In specific cases, such as law enforcement activities, these rules must be applied side-by-side with sector regulations. Consent is the standard legal basis for data processing by public authorities. However, the law establishes various exceptions that allow data usage without such consent. The main exception to the rules set by the LGPDSSO is data processing for national security purposes, which is regulated by the National Security Law (NSL) from 2005, which has fewer provisions on data protection. Adequate protection for individuals in situations of government access requires that different Mexican oversight authorities maintain their independent status, free from political interference.

Türkiye recognises both the right to privacy and the right to personal data protection as a fundamental right in its constitution. This protection extends to all individuals, including foreigners, and includes rights such as the right to be informed, access, rectification, and the right to be forgotten. While the Turkish Data Protection Law (TPDPL) provides secondary-level protection for personal data, it exempts judicial authorities, law enforcement, and intelligence organisations from its scope. National security and law enforcement authorities process personal data therefore without a specific legal framework, though they are still bound by any limits posed by the Constitution. Moreover, specialised laws have put in place specific safeguards and oversight mechanisms. Individuals can seek redress through *ex-post* judicial and individual complaints of violation of privacy and data protection rights before the Constitutional Court. Yet, the proportionality of governmental access can be questioned based on four concerns: (i) the necessity and proportionality of the substantial and procedural conditions for such access; (ii) the safeguards for citizens abroad and foreigners; (iii) the independence of the different oversight mechanisms; and (iv) the adequacy of the implementation of data subject rights in Turkish law.

1 INTRODUCTION

1.1 OBJECTIVES AND SCOPE OF THE STUDY

According to Article 46 of the General Data Protection Regulation (GDPR)¹, data controllers and processors may transfer personal data to third countries or international organisations only if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Whereas it is the primary responsibility of data exporters and data importers to assess that the legislation of the country of destination enables the data importer to comply with any of the appropriate safeguards, supervisory authorities (SAs) play a key role when issuing further decisions on transfers to third countries. Hence, this report provides the European Data Protection Board (EDPB) and the SAs in the EEA/EU with information on the legislation and practice in Mexico, and Türkiye on their governments' access to personal data processed by economic operators. The report contains an overview of the relevant information in order for the SAs to assess whether and to what extent legislation and practices in the abovementioned countries imply massive and/or indiscriminate access to personal data processed by economic operators.

In order to answer the research questions, the study has

- investigated the general situation of Mexico, and Türkiye with regard to the protection of fundamental rights and freedoms, by analysing international reports and findings from public bodies (e.g. Council of Europe, UN Human Rights Council and Human Rights Committee) and renowned non-governmental bodies (e.g. Amnesty International, Human Rights Watch, Privacy International). To this end, the study also identified the countries' international commitments in the field of human rights, in particular of the right to privacy and data protection;
- analysed the legislation of the countries in order to establish the substantive and procedural conditions for government access to personal data, including law enforcement and intelligence agencies. Specific attention was paid to the authorities involved in the adoption or amendment of the related rules, and entitled to authorise the governmental access to personal information;
- investigated whether specific purposes and conditions to access personal data of foreign individuals exist in both countries;
- identified, where existing, oversight mechanisms with regard to the governmental access to personal data, and to assess the independency from the executive of the bodies empowered to perform such control; and
- focused on rights and administrative or judicial redress mechanisms that are available to data subjects (including foreign individuals) in the observed countries.

The study is not limited to an up-to-date overview of relevant legislation and case law, but also contains information with regard to the implementation of the legislation in the both countries in practice, which has mostly been collected through interviews.

1.2 LEGAL BACKGROUND

This section gives an overview of the legal framework for assessing governmental access to personal data in a third country from the perspective of EU law, where such an assessment is required in the

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

context of international personal data transfers under the GDPR². The main legal instruments considered are the EU-Charter of Fundamental Rights of the EU (EU-Charter), the European Convention of Human Rights (ECHR) and the GDPR³.

1.2.1 DATA TRANSFERS IN THE GDPR

Personal data transfers to a third country or to an international organisation under the GDPR are only permitted if they comply with the requirements of Chapter V⁴. In principle, the GDPR allows the transfer of personal data to third countries or to international organisations based on three broad transfer tools, namely: (i) adequacy decisions; (ii) appropriate safeguards, i.e., legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, standard contractual clauses, codes of conduct, or certification mechanisms⁵; and (iii) derogations⁶. With these tools, the GDPR intends to provide a high level of protection to personal data transferred to third countries and international organisations⁷. Accordingly, the third country, international organisation or the transfer instrument, in case of appropriate safeguards, should provide guarantees, safeguarding a level of protection essentially equivalent to that ensured within the Union⁸. The Court has gradually developed the criteria for essential equivalence in *Schrems I*, *Opinion 1/15*, and *Schrems II*, which are relevant for all transfer mechanisms provided in the GDPR⁹.

1.2.2 INTERFERENCES WITH THE FUNDAMENTAL RIGHTS UNDER THE EU-CHARTER

Governmental access to personal data transferred from the EU to a third country or international organisation has been found by the CJEU to constitute an interference with Articles 7 (right to privacy), 8 (right to data protection), 21 (non-discrimination) and 47 EU-Charter (right to an effective remedy and fair trial). First, if communication data (content and/or meta-data) are maintained, accessed, and/or exposed by public authorities at the transfer's destination, this can constitute an interference with the fundamental right to privacy in Article 7¹¹. Second, there can be an interference with Article 8, when the transfer of personal data constitutes processing of such data¹⁰. Third, due to “*the risk of data being processed contrary to Article 21 of the Charter*,” the CJEU decided in *Opinion 1/15* that the transfer of special categories of personal data would require a precise and particularly solid justification¹¹. Fourth, the lack of effective remedies in a third country or international organisation in a situation of

² Article 46 GDPR.

³ Article 52(3) of the EU Charter states “*in so far this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.*” Therefore, the sought assessment needs to take place following the interpretation of both the CJEU and the European Court of Human Rights (ECtHR).

⁴ Article 44 GDPR.

⁵ Articles 46 and 47 GDPR.

⁶ Article 49 GDPR.

⁷ Article 44 GDPR ‘to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined’.

⁸ Recital 104 GDPR.

⁹ Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650, paragraph 64; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 105 and 188. The *Schrems II* decision is the first to explicitly address the issue of the level of protection necessary for international data transfers under the different transfer mechanisms of the GDPR. In this case, the Court clarified the connections between the various mechanisms and ruled that they should be all afforded essentially equal levels of protection to those provided by the GDPR. See judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 92.

¹⁰ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 124; and its paragraph 126: “*Those operations also constitute an interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the EU Charter since they constitute the processing of personal data*”; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 170 and 171; and its paragraph 83: the “[...] the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data [...]”.

¹¹ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 165; judgment of the Court of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 181.

governmental access can interfere with the fundamental right to an effective remedy in Article 47¹². However, none of the mentioned fundamental rights are absolute rights, thus where necessary, they can be limited following strict conditions listed in Article 52(1) of the EU-Charter.

According to Article 52(1) of the EU-Charter, an interference with a fundamental right can be justified, if it is (i) provided by law and (ii) respects the essence of the right, meaning that the interference must not empty the right of its core elements and prevent the exercise of the right. Furthermore, the interference must (iii) genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; and finally, (iv) it must be necessary and proportionate¹³.

1.2.3 LEGALITY OF GOVERNMENTAL ACCESS

According to Article 52(1) of the EU-Charter, any interference to a fundamental right of the EU Charter must be **provided for by law**. The CJEU holds that “*the legal basis which permits the interference [...] must itself define the scope of the limitation on the exercise of the right concerned*”¹⁴. The national laws permitting the interference shall lay down clear and precise rules governing the scope and application of the limitation¹⁵. As dissected in its elements below, the quality of law requirement is the first step when assessing if the interference is compatible with the EU-Charter¹⁶.

First, the law authorising the interference, e.g., the governmental access, must be “*accessible to the persons concerned and foreseeable as to its effects*”¹⁷. Foreseeability refers to the formulation of the law with sufficient precision to enable persons to regulate their conduct¹⁸. The level of such precision depends on the particular subject-matter¹⁹. For example, in the particular context of secret measures of surveillance, such as interception of communications, foreseeability cannot mean that individuals should be able to foresee when the authorities are likely to intercept their communications so that they can adapt their conduct accordingly²⁰. However, when executed secretly, the power granted to such secret activities may risk arbitrariness²¹.

In *Schrems II*, when assessing the US surveillance programme, the CJEU stated that “[...] *the legislation*

¹² Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 227. Although in this case, the interference with the PNR agreement was not found to be in violation with Article 47. See further judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 186.

¹³ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 124; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 82, 170-171.

¹⁴ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 227. Although in this case, the interference with PNR agreement was not found to be in violation with Article 47. See further judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 186.

¹⁵ Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 180.

¹⁶ The meaning of the expression ‘provided for by law’ should be in line with the ECtHR case law, which is frequently cited by the CJEU: an interference shall be based on a provision of law that has certain qualities, also known as the “quality of the law” requirement (judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, EU:C:2016:970; Opinion of Advocate General Saugmandsgaard delivered on 19 July 2016, paragraph 40). The CJEU has referred to a body of ECtHR case law in *La Quadrature du Net*, paragraph 128 in this regard: “*a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected*” (ECtHR, 28 October 1998, *Osman v. United Kingdom*, no. 23452/94, paragraphs 115 and 116; ECtHR, 4 March 2004, *M.C. v. Bulgaria*, no. 39272/98, paragraph 151. See also: ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 276).

¹⁷ ECtHR, 4 December 2015, *Zakharov v. Russia*, no. 47143/06, paragraphs 228-230; ECtHR, 16 February 2000, *Amann v. Switzerland*, no. 27798/95, paragraph 50; also see EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*, pp. 6-7.

¹⁸ ECtHR, 16 February 2000 *Amann v. Switzerland*, no. 27798/95, , paragraph 56; ECtHR, 2 August 1984, *Malone v. the UK*, , no. 8691/79, paragraph 66.

¹⁹ ECtHR, 26 April 1979, *The Sunday Times v. the UK*, no. 6538/74, paragraph 49.

²⁰ ECtHR, 18 May 2010, *Kennedy v. the United Kingdom*, no. 26839/05; , ECtHR, 29 June 2006, *Weber and Saravia*, no. 54934/00, paragraphs 152, 93-95.

²¹ ECtHR, 2 August 1984, *Malone v. the United Kingdom*, no. 8691/79, , paragraph 67; ECtHR, 24 April 1990, *Huvig v. France*, no. 11105/84, paragraph 29.

*in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question [...].*²² The possibility that the surveillance programmes allow access to data (even to data in transit) without sufficiently clear and precise limits was considered a violation of the legality of the governmental access²³. Such a law needs to have explicit, detailed provisions on surveillance procedures, providing individuals with a sufficient indication regarding the situations in which public authorities may execute surveillance measures and the conditions thereof²⁴. As will be further explained below, the legality of the interference is closely related to whether the limitation is necessary and proportionate²⁵.

1.2.4 OBJECTIVES OF GENERAL INTEREST OR PROTECTION OF RIGHTS AND FREEDOMS OF OTHERS

Governmental access needs to be strictly necessary to comply with **an objective of general interest or to protect the rights and freedoms of others**²⁶. An objective of general interest cannot be sought without considering how it must be reconciled with the fundamental rights impacted by the legislation. This is done by appropriately balancing the general interest goal against the rights in question²⁷. Therefore, the objective of general interest and the necessity and proportionality of the limitation are closely associated; it is essential to define and clarify the objective of general interest aimed by the limitation in satisfactory detail, as the necessity and proportionality test will be carried out against this context²⁸.

In that regard, it is worth referring to the case law of the CJEU on data retention, which discusses both the retention of personal data by private operators in order to be accessed by governmental authorities, and the conditions of such access²⁹. It is clear from the Court's case law that only the national security objective may justify public authorities having broad access to retained personal data in a general and indiscriminate manner (bulk access)³⁰. The national security objective must be linked to a genuine and present or foreseeable serious threat³¹.

²² “*It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted [...]*” judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 176.

²³ Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 180; see also judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650.

²⁴ ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 370.

²⁵ ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 334.

²⁶ Article 3 of the Treaty on the European Union, for instance, mentions freedom, security, and justice as general objectives. EDPB (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, p. 11. Article 23 of the GDPR states that data protection can legitimately be limited for security, defence, crime prevention, significant economic and financial interests, public health and social security, provided that the limitation respects the essence of the right to personal data protection and is necessary and proportionate. See also EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*. Relatedly, the CJEU in *Schwarz v. Stadt Bochum* found that processing personal data to prevent illegal entry to the EU pursued an objective of general interest (judgment of the Court (Fourth Chamber) of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670).

²⁷ Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, paragraph 52; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130.

²⁸ EDPS (2017), *Necessity toolkit*, p. 4.

²⁹ See *Privacy International*, paragraph 73: “*the mere retention of that data by the providers of electronic communications services entails a risk of abuse and unlawful access.*”

³⁰ Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, paragraph 31; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 166.

³¹ Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, paragraph 58; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168.

Targeted access to and retention of traffic and location data are considered by the CJEU to be a serious interference, thus such targeted access must be based on objective evidence which makes it possible to target individuals whose traffic and location data are likely to reveal a direct or indirect link with serious criminal offences³². Objective evidence has to be non-discriminatory, e.g., a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending³³. Moreover, on the basis of objective and non-discriminatory criteria, geographical areas characterised by a high risk of preparation for, or commission of serious criminal offences can be targeted.

An interference with fundamental rights of the EU Charter can also be justified if it is necessary to protect the rights and freedoms of others. The right to personal data protection often ambivalently interplays with other rights, such as freedom of expression and the right to receive and impart information. In such cases, courts must carry out a balancing exercise to settle the tension between the two³⁴.

1.2.5 NECESSITY AND PROPORTIONALITY

Fundamental rights and freedoms of the EU can be interfered with only if this is strictly necessary³⁵. This translates into the requirements of necessity and proportionality³⁶. Proportionality requires a balance to be struck between the importance of the public interest pursued and the seriousness of the interference with fundamental rights³⁷. Pursuant to the CJEU, proportionality necessitates the presence of minimal safeguards, such as enforceable rights and effective judicial review, in order to guarantee that interferences are “limited to what is strictly necessary”, as stated in *Schrems II*³⁸. Apart from the cases directly related to international personal data transfers, the CJEU has developed criteria on how to handle the necessity and proportionality assessments in its case law on data retention mentioned above³⁹. This case law should be considered relevant also for international personal data transfers that result in governmental access because it explains the limits to such access from the perspective of the EU-Charter⁴⁰.

The proportionality assessment extends to the access to and the use of retained data, which should also be limited to what is strictly necessary for the investigation⁴¹. Authorisation must be asked prior to

³² Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111 and judgment of the Court (Grand Chamber) of , 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18, and C-520/18, EU:C:2020:791, paragraph 148.

³³ Judgment of the Court (Grand Chamber) of 5 April 2022, C-140/20, *G.D. v The Commissioner of the Garda Síochána and Others*, EU:C:2022:258, paragraph 78.

³⁴ For example, the GDPR Article 85 states that the Member States shall reconcile by law the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic, academic, artistic, and literary expression. Freedom of expression and information is ensured by Article 11 of the EU Charter, and limitations on this right must fulfil the criteria in Article 52 (1), provided above. To achieve a balance between two fundamental rights, the limitations of the right to data protection must apply only insofar as strictly necessary (judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727, paragraphs 56-62).

³⁵ Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 176 and Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 140-141.

³⁶ According to the EDPS, the necessity test requires “*a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal*” (EDPS (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*, p. 27, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf). For other views on necessity see: Gerards, J., ‘How to improve the necessity test of the European Court of Human Rights’, *International Journal of Constitutional Law*, Vol. 11, No 2, April 2013, pp. 466–490, available at: <https://doi.org/10.1093/icon/mot004>.

³⁷ Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 130-131.

³⁸ Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 184.

³⁹ Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 35.

⁴⁰ EDPR (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, p. 7.

⁴¹ Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, paragraph 38.

access to the data, except in the event of a justified urgency⁴². This review must be carried out either by a court or an independent administrative body whose decision is binding. Moreover, means for individuals to obtain effective judicial and administrative redress should be in place⁴³. Data subjects need an effective possibility to access the retained data, obtain rectification, or erase data⁴⁴.

The ECtHR has developed minimum safeguards that the national law authorising governmental access should contain in the cases *Weber & Saravia v. Germany*,⁴⁵ *Roman Zakharov v. Russia*, and *Big Brother Watch and the Others*⁴⁶. Such laws need to include clear provisions on:

- the nature of offences that may give rise to a limitation;
- the categories of people liable to have their communications intercepted;
- a limit on the duration of interception;
- the procedure to be followed for accessing, examining, using and storing, communicating and destroying the data obtained;
- the precautions to be taken when communicating the data to other parties and the circumstances in which intercepted data may or must be erased or destroyed; and
- the review of the authorisation procedures and arrangements supervising the implementation of the measures along with any notification mechanism and the remedies provided⁴⁷. This last safeguard may come into play when (i) the surveillance is first ordered, (ii) while it is being carried out, or (iii) after it has been terminated⁴⁸.

1.2.6 RESPECT THE ESSENCE OF THE RIGHT

In some instances, an interference can be so extensive and invasive it empties an EU fundamental right of its essence⁴⁹. In this regard, the CJEU considered the law allowing public authorities to access, on a general basis, the content of electronic communications as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the EU-Charter⁵⁰. However, in *Digital Rights Ireland*, where the legislation in question did not permit generalised access to content data, the CJEU held that the limitation was not so intrusive as to impact the essence of the right⁵¹. *Schrems I* noted that legislation that does not provide any possibility to pursue legal remedies, e.g., access to or to rectify personal data, would be incompatible with Article 47 of the EU-Charter, ensuring the fundamental right

⁴² Judgment of the CJEU (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 120; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 137-139; judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratoraat*, C-746/18, EU:C:2021:152, paragraphs 40,53-54,58; ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 355.

⁴³ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 218-227.

⁴⁴ *Ibid*. See further judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 190.

⁴⁵ ECtHR, 29 June 2006, *Weber and Saravia*, no. 54934/00, also mentioned in judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 175; judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International*, C-623/17, paragraph 65.

⁴⁶ ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 54.

⁴⁷ ECtHR, 4 December 2015, *Zakharov v. Russia*, no. 47143/06, paragraphs 228-230; ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 335.

⁴⁸ ECtHR, 25 May 2021, *Big Brother Watch*, paragraph 336.

⁴⁹ Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 124, 138-141, 150; EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*, p. 6.

⁵⁰ Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14 EU:C:2015:650, paragraph 94.

⁵¹ Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39.

to effective judicial protection⁵².

The essence of a right is interpreted by legal scholars in two ways. The first approach reads the notion as an absolute limit which is not subject to balancing⁵³. Following the first view, where the essence of a fundamental right is violated, the interference is unlawful without a further need for testing its necessity and proportionality⁵⁴. The second view links the essence to proportionality test as explained above⁵⁵. In this view, essence forms one component in the proportionality test.

1.3 STUDY METHODOLOGY

For this study, a literature review via desk research (books, journal articles, databases and other online sources) was conducted as the primary step. The purpose of this review was to map the law in the books, consisting of the relevant legal instruments and relevant case law. In addition, reports of international organisations were compiled in this step. After conducting a legal analysis of the collected sources, the loopholes in the knowledge in this area of law were defined for each country (Mexico, and Türkiye). Thereafter, focus was laid on the law in action. Per country, a customised questionnaire was composed, tackling the higher defined loopholes (see Annex 1). Both country questionnaires were priorly presented to the EDPB, making it possible to distribute the questionnaires to carefully selected experts in each country. To have a broad perspective, the researchers of this study strived to find persons working in different legal fields (academia, non-profit sector, the Bar ...).

We have carried out the following numbers of interviews:

- Mexico: five stakeholders were interviewed, including four lawyers and one representative of academia. The interviews were crucial to understand the Mexican federation system, the different functions of the data protection authorities, and the difference between the legal rules and their application, which has been indicated in the footnotes.
- Türkiye: five stakeholders were interviewed, including three representatives of academia and two practising lawyers from different law firms. The interviews have largely validated the already collected information. The interviews contributed to a better understanding of upcoming legislation, as some of the interviewees had been involved in this process.

Finally, the interviews were carefully analysed and compared with the results of the desk research. Where needed, anomalies were indicated. Based on this, the end report of the in-depth analysis of the countries was drafted including the results of the interviews.

⁵² Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650, paragraphs 64 and 95. The same conclusion regarding Article 47 was reached in *Schrems II*, where the Court stated: “According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter” (judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 187).

⁵³ “From a methodological perspective, the case law of the CJEU reflects the fact that court will first examine whether the measure in question respects the essence of the fundamental rights at stake and will only carry out a proportionality assessment if the answer to that first question is in the affirmative”. Lenaerts, K., ‘Limits on Limitations: The Essence of Fundamental Rights in the EU’, *German Law Journal*, Vol. 20, pp. 787, 779-793, Cambridge University Press, 2019. See further Brkan, M., ‘The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU’s constitutional reasoning’, *German Law Journal*, Vol. 20, pp. 864-883, Cambridge University Press, 2019.

⁵⁴ European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018, p. 44.

⁵⁵ Tridimas, T., Gentile, G., ‘The essence of Rights: An Unreliable Boundary?’, *German Law Journal*, vol. 20, pp. 794–816 and itsp. 804: “In short, although the concept of essence as a legal threshold must be understood as an autonomous limit, in effect, it is impossible to determine it without engaging in a balancing process which is best carried out through a proportionality analysis.”

1.4 STRUCTURE OF THIS REPORT

Section 2 describes an in-depth analysis of the legislation and practice on government access to personal data in Mexico (section 2.1) and Türkiye (section 2.2). The same structure is followed in every country section.

Each country section presents a first subsection aiming to answer the research question concerning the general situation of the countries as regards human rights, and specifically the right to privacy and data protection. It provides an overview concerning the rule of law, respect for human rights and fundamental freedoms in the observed countries. The main constitutional provisions of both countries are analysed, as well as the concrete application of such provisions in the national case law. The subsection also illustrates whether and how the right to privacy exists in both legal systems. Afterwards, the general findings by international organisations on the the countries' human rights situation are also briefly shown.

Subsequently, the country reports include a subsection illustrating the purposes, conditions, and oversight mechanisms of the governmental access to personal data in both countries. This subsection aims to answer the research questions related to the specific legislative requirements for government access to personal data; where specific provisions on foreign individuals' personal data do not always exist in the legal systems, the report also tries to address the research questions around the applicability of the countries' legislation to foreigners.

In each country section, a subsection is dedicated to the data subjects' rights, their conditions for applicability and the redress mechanisms available to enforce them. The subsection's goal is to answer the research questions around individual rights and existing redress mechanisms as regards the right to privacy in the legal systems of both countries.

Section 3 provides conclusions by answering the research questions.

The annexes included to this study entail the exact questionnaires per country (Annex 1), a list of all the used sources (Annex 2) and an overview of the used acronyms and abbreviations (Annex 3).

2 IN-DEPTH ANALYSIS OF THIRD COUNTRIES

The following section aims to answer the research questions of the study in relation to both countries. The structure of the subsections is consistent with a division into areas of interests touched upon by the research questions. The answers are integrated in the related subsections. Each section provides an in-depth analysis of the legislation and practice in third countries on their governments' access to personal data. Section 2.1 deals with the situation in Mexico and Section 2.2 with Türkiye. All these sections study the situation in third countries from the perspective of the rule of law and respect for human rights and fundamental freedoms; government access to personal data; and data subject rights. Any potential upcoming changes in the legislation are also discussed. Finally, every country section contains an intermediary conclusion and a grid visually presenting the research results.

2.1 MEXICO

2.1.1 RULE OF LAW, RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

Mexico is a presidential representative democracy and a constitutional republic. The Mexican Constitution dates from 1917 and there were several amendments throughout the years – the last one being published at the end of 2022.

Privacy has been a fundamental right in the Mexican constitution since its initial text. The right to personal data protection, however, was only included in the Mexican constitution in 2004. The amendment consisted of provisions stating that every person has free access to their personal data and the possibility to rectify their information without justification. In 2017 a specific provision mentioning the right to data protection was added to the constitution.

The constitutional text already sets a list of minimum individual rights that should apply to all processing of personal data. These are the ARCO rights, namely access, rectification, cancellation, and objection to processing⁵⁶. Another individual right is the possibility to oppose the disclosure of personal data. The ARCO and other data protection rights are constitutional, thus applied to every person, regardless of their nationality. Any restriction to these individual rights must be justified by reasons of national security, law and order, public security, public health, or the protection of fundamental rights of third parties. Such limitations are implemented by a specific law – the National Security Law (NSL)⁵⁷. Reaffirming the general aspect of the right to data protection, the Mexican Supreme Court ruled that the principles of data protection apply when data are shared with a public authority⁵⁸.

The constitution requires that Mexico establishes an autonomous, specialised, impartial, and independent authority to be responsible for transparency and access to public information and data protection. Such an authority is then responsible to oversee the data processing controlled by private and public parties (Article 5, VIII Constitution). Based on this provision, the National Institute for Transparency, Access to Information and Data Protection (INAI)⁵⁹ was created. The body has published many guidelines and recommendations, such as the Guidelines for the Processing of Biometric Data⁶⁰. Besides its normative work involving publishing guidelines and other documents, the INAI issues yearly reports on the activities it carries out⁶¹.

The role of the guidelines issued by the INAI differs depending on to whom they are addressed. Guidelines for the public sector should be observed, considering the INAI's role as a second instance of oversight of data protection activities. But documents that address private parties are non-binding and cannot be used in court, as ruled by the Supreme Court. The Supreme Court clarified that “[...] it is possible to determine that the INAI is only entitled to issue internal administrative regulations or ordinances with purposes to regulated aspects related to its functioning and operation, is strict

⁵⁶ Article 16, §1, Mexican Constitution establishes: “All people have the right to enjoy protection of his/her personal data, and to access, correct and cancel such data. All people have the right to oppose the disclosure of his/her data, according to the law. The law shall establish exceptions to the criteria that rule the handling of data, due to national security reasons, law and order, public security, public health, or protection of third party's rights.”

⁵⁷ Ley de Seguridad Nacional, de 31 de enero de 2005.

⁵⁸ Case n. 2005522, Thesis P. II/2014, 21 January 2014, summary of the decision: “Judicial persons. They have the right to the protection of the data that may be equal to personal data, even if such information has been delivered to a public authority.”

⁵⁹ Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

⁶⁰ Available at: https://inicio.inai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf.

⁶¹ INAI, Informe de Labores 2022, available at: <https://micrositios.inai.org.mx/informesinai/>.

congruence with the constitutional text, especially since it does not have the power to legislate on the substantive matter of protection of personal data held by private companies”⁶².

Internationally, Mexico has a strong presence in Conventions regarding human rights. The country has ratified the Universal Declaration of Human Rights, the International Convention on Civil and Political Rights, the International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families and Convention 108 and its additional protocol. More recently, the country has signed the OECD’s “Declaration on Government Access to Personal Data Held by Private Sector Entities”⁶³. Regionally, Mexico has ratified the American Convention on Human Rights, and is part of the Inter-American Court of Human Rights.

The country’s legal system is based on civil law and codified laws. Data protection is regulated by two main laws – one focused on the private sector and the other one on the public. For companies (the private sector), the Law on the Protection of Personal Data in the Possession of Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares* - LFPDSSPP) became applicable in 2010. The LFPDSSPP sets out a series of principles and procedures that should be observed by controllers of personal data; it already establishes that the principles and rights foreseen in the law can be limited for purposes of national security, public order, security, health, and third parties’ rights⁶⁴.

After seven years, to avoid a legal gap in cases where the LFPDSSPP does not apply, the Law on the Protection of Personal Data in the Possession of Public Parties (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* - LGPDSSO) was adopted in 2017. The law applies to any federal, state, or municipal public body, including every authority of the executive, legislative and judicial powers, political bodies, and public funds, including law enforcement authorities. Thus, differently from what is regulated by the LFPDSSPP, the LGPDSSO applies directly to the public sector. Following the constitutional provisions, the law reaffirms that the right to data protection may only be limited for purposes of national security⁶⁵, public order, security, health, and to protect third parties’ rights⁶⁶.

The LGDPSSO also addresses the right to access public data, mentioning the National System of Transparency, Access of Information and Data Protection⁶⁷. This shows the importance of the General Law of Transparency and Access to Public Information (*Ley General de Transparencia y Acceso a la Información Pública* - LGTAIP). The LGTAIP establishes common rules to public authorities when implementing the principle of transparency. The law also addresses some proportionality issues related to access to public data and the fundamental right to protection of personal data.

According to the interviewed national experts, the National Code of Criminal Procedures is the most relevant law on regulating surveillance activities carried out by law enforcement authorities⁶⁸. Additionally, Mexico has a National Security Law (NSL), which, as mentioned above, sets rules on data processing for national security purposes. Thus, there is no legal gap on data processing for these purposes, since the NSL establishes the rules for these activities.

Mexico is a federation; thus, various levels of legal and government systems co-exist⁶⁹. This can lead to difficulties when implementing legal reforms by the Mexican federal government, especially in the field of human rights. With the involvement of international bodies and civil society, new regulations bring

⁶² Amparo Directo en Revisión 6489/2018.

⁶³ The complete text of the document is available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

⁶⁴ Article 4 of the LGPDSSPP.

⁶⁵ Usually, intelligence activities fall under this exception.

⁶⁶ Article 6 of the LGPDSSO.

⁶⁷ Sistema Nacional de Transparencia, *Acceso a la Información y Protección de Datos Personales*.

⁶⁸ Interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.

⁶⁹ Mexico has 33 jurisdictions, composed of 31 states, Mexico City and a federal jurisdiction.

obligations to all levels of government, including rules of transparency in public authorities and data protection. The new developments bring more uniformity to the Mexican legal system⁷⁰.

In terms of legislation, the fact that Mexico is a federation is noticeable in the different types and levels of legislation⁷¹. In states and municipalities, local laws can be developed. National Congress can publish federal, general or national laws. Federal laws are adopted in accordance with the competences attributed to the National Congress. General laws outline the regulation of a topic determined by the Constitution, harmonising the system while dividing competences. Federal entities must observe the provisions set by the general law, even when legislating on the details of the topic. Other levels of laws cannot modify what is established by the general law. National laws are always linked to the constitutional attribution of the distribution of competences⁷².

The characteristics of the federal system are also visible in the regulation and oversight of data protection. Regarding processing activities carried out by public authorities, the general law (LGPDSSO)⁷³ establishes general guidelines that shall be observed by local levels, while dividing competences⁷⁴. Nonetheless, each federal entity incorporates the general rule locally, determining how the provisions and competences set by the LGPDSSO will be applied locally⁷⁵. Based on the federal constitution⁷⁶, each local constitution or law also establishes an authority responsible for overseeing the data processing and transparency activities carried out by public entities in that region, while the local authorities' activities are assessed by the INAI. This system is reaffirmed by the LGPDSSO.

Personal data processed by private entities is a federal competence⁷⁷, this means that there are no local laws on the matter⁷⁸. Therefore, the INAI is the competent authority to oversee the data processing activities by private parties, not dividing this competence with local bodies. However, a ruling from the Supreme Court stated that the constitutional provision that foresees this competence (Article 73, XXIX-O) does not include the power to issue general and abstract rules on this topic. The National Congress is the body responsible for such rules⁷⁹.

Considering the impossibility of analysing in detail all the different regional and local legislations, this study focuses on the general laws and on the LGPDSSP. Regarding other topics that are relevant to the scope of the study, the different types of laws are taken into account. Such an approach addresses the

⁷⁰ García, A., *Transparency in Mexico: An Overview of Access to Information Regulations and their Effectiveness at the Federal and State Level*, 2016, Report, Wilson Center Mexico Institute.

⁷¹ The Supreme Court ruled that there are five different legal orders in Mexico: “the federal, the local or state, the municipal, the Federal District, and the Constitutional”, Suprema Corte de Justicia, Controversia Constitucional, P.J., 136/2005.

⁷² Estrada, J. M. M., ‘Configuración normativa de las leyes en el marco competencial de los órdenes jurídicos’, *Congreso Redipal Virtual VIII*, Marzo 2015, available at: <https://www.diputados.gob.mx/sedia/sia/redipal/CRV-VIII-14-%202015.pdf>; Tópez, S.T.,’Sustitución de la Ley Federal de Archivos de México: el alcance de una ley general’, *Revista Española de la Transparencia*, no 12, Jan-Jun 2021, Estado de México, Periódico Oficial Gaceta del Gobierno y Legistel, Leyes Nacionales, Generales y Federales, pp. 167-187, available at: https://legislacion.edomex.gob.mx/leyes_federales.

⁷³ Article 73 Mexican Constitution: “The Congress shall have the power to: XXIX-S. To issue general regulating laws that establish the principles and basis in regard to government transparency, access to information and protection of personal data held by authorities, entities or government agencies at all levels of government.”

⁷⁴ One of the objectives of the LGPDSSO is to distribute competences between the federal and local oversight authorities in matter of data protection processed by public entities (Article 2, I, LGPDSSO).

⁷⁵ Article 9, §1, Mexican Constitution.

⁷⁶ Article 116, VIII, Mexican Constitution: “The local constitutionas shall establish specialised, impartial, collegiate and autonomous entities responsible for guarantee the right of access to information and the protection of personal data held by public parties, following the principles and fundamental established in the Article 6 of this Constitutional and the general basis, principles and procedures to exercise these rights stated by the general laws issued by the Mexican Congress”.

⁷⁷ Lopes, T. M. G., ‘Las recientes reformas em materia de protección de datos personales em México’, *Anuario Jurídico y Económico Escurialense*, XLIV, 2011, ISSN: 1133-3677, Mexico, pp. 317-334.. Lineamientos Generales de Protección de Datos Personales para el Sector Público, available at:

https://www.gob.mx/cms/uploads/attachment/file/304930/lineamientos_generales_para_la_protecci_n_de_datos_personales_para_el_sector_p_blico.pdf.

⁷⁸ Article 73 Mexican Constitution: “The Congress shall have the power to: XXIX-O. Regulate the use and protect personal data handled by private entitites”.

⁷⁹ Amparo Directo en Revisón 6489/2018.

main objective of the work, especially since the general laws shall be transposed in the regional regulations. Therefore, this approach allows the evaluation of the main provisions in Mexico, while also giving an overview of the topics that are further regulated locally. The following table summarises the laws evaluated in this work and the different legal scopes:

Law	Year of publication	Scope	Local and federal legislations?
Ley de Seguridad Nacional	2005	General	No
Ley Federal de Protección de Datos Personales en Posesión de los Particulares	2010	Federal	No
Código Nacional de Procedimientos Penales	2014	Federal and local judicial bodies	Yes ⁸⁰
Ley General de Transparencia y Acceso a la Información Pública	2015	General	Yes
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	2017	General	Yes

2.1.1.1 TRANSPARENCY RULES AND DATA ACCESS

Since 2002, state laws have been in force in different Mexican regions on transparency and data access. In 2007, Article 6 of the Constitution was amended to regulate the principle of transparency and the right to access information⁸¹. The General Law for Transparency and Access to Public Data (LGTAIP)⁸² was created in 2015 to implement the constitutional provisions about the principle of transparency and access to information in the public sector. Following the Mexican legal system, this general law establishes minimum bases for the topic of transparency and access to public data, while dividing competences with states and the Federal District. Thus, there are regional laws operationalising the general law.

The final text of the LGTPAI was the result of the work of a multisector group established by Congress, which provided for stricter provisions on judicial and societal control over the government's activities. The fact that corruption is put as one of the scenarios where information cannot be withheld, considering all the previous claims of human rights' violations, exemplifies this scenario. Another relevant provision is the obligation of publicising the rulings of the Mexican Courts, especially the binding ones. The law also increased the competences of oversight bodies. Each state, Mexico City and the federal government had to create an independent and specialised oversight authority to guarantee compliance with the provisions on transparency. The federal authority is the INAI.

This scenario led to the creation of the National Transparency System⁸³. Its role is to coordinate and evaluate the actions related to transparency, access to information, and personal data protection, and to establish and implement criteria and guidelines⁸⁴. For this, the System is also responsible for organising the use of the National Transparency Platform (*Plataforma Nacional de Transparencia*), while promoting the right to access to public information and personal data for the purposes of the LGTAIP.

⁸⁰ The Code of National Procedures harmonises the criminal procedures throughout the whole country, for local or federal judicial bodies, thus, federal or local crimes. However, local criminal codes still exist. Mexico, Senado de la República, Código Nacional de Procedimientos Penales, 2014, available at: senado.gob.mx/comisiones/justicia/docs/CNPP.pdf.

⁸¹ These provisions follow the principle of maximum disclosure, defined by Article 8, VI, of the LGTAIP as “*every information in the control of public authorities must be public, complete, timely and accessible, subjected to an exception regime that must be defined and legitimate and strictly necessary in a democratic society*”.

⁸² Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

⁸³ Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

⁸⁴ Article 28, LGTAIP.

The following bodies are part of the National Transparency System⁸⁵:

- the INAI;
- the local oversight bodies⁸⁶;
- the General Auditor's Office (*la Auditoría Superior de la Federación*);
- the National General Archive (*el Archivo General de la Nación*); and
- the National Institute for Statistics and Geography (*el Instituto Nacional de Estadística y Geografía*).

Even though the main oversight focus is related to the management of public assets, the use of personal data is also a topic of discussion in the LGTPAI. The need for balancing the rights of access to information and data protection is acknowledged in the law⁸⁷. Thus, while developing their activities, public authorities must consider the protection of personal information in parallel to transparency rules. Non-personal data is to be accessible, except for a determined period and for reasons of public interest or national security⁸⁸. With these considerations, public authorities may decide on data access requests. Their decision can be subject to a revision claim (*recurso de revisión*).

In fact, any individual can make a revision claim in front of the local competent authority. The LGTAIP established that the following topics can be discussed in such claims:

- classification of information (confidential, reserved or public);
- declaration of inexistence of the information;
- declaration of incompetence by the public authority;
- providing incomplete information;
- delivering different information to what was requested;
- lack of response of an access request in time;
- delivering of information in a different format to the requested;
- the costs or time frame for the access of information;
- lacking a procedure for a request;
- denying direct consultation to the information;
- insufficient justification in the response of the public authority; or
- the rules published by a public authority on a specific procedure, e.g. for the right of access.

Other topics may be discussed in revision claims as long as they relate to the right of access to public information. To do this, the individuals should justify their claims on the basis of the LGTAIP or other relevant legislation, including national and international rulings or opinions on transparency⁸⁹.

The revision claims will then be analysed by the competent authority. Actions of federal bodies should be presented to the INAI. In other instances, activities of state or municipal bodies will be overseen by the local authorities. The system has the local oversight bodies as the first instance, since all the decisions of these bodies are overseen by the INAI⁹⁰. Judicial bodies can overturn and supervise the decisions

⁸⁵ Article 30 LGTAIP; Article 31 of LGTAIP establishes all the functions of the National System.

⁸⁶ Each federal entity has to establish an autonomous authority for transparency and data protection. The INAI acts for the federal level. However, there are 31 state authorities and one authority for the Federal District.

⁸⁷ Article 23 of the LGTAIP “*The following entities are obliged to publish and allow the access to information and to protect the personal data under their control: any authority, entity, body or organ of the Executive, Legislative and Judicial Power, autonomous bodies, political parties, fiduciaries and public funds, as any other person – private or legal – or union that receives and uses public assets or perform authority activities in federal, state or municipal scope.*”

⁸⁸ Article 4 of the LGTAIP. However, information related to severe violations of human rights or to crimes against humanity can never be classified as reserved.

⁸⁹ Article 7 paragraph 2 LGTAIP “*For interpretation purposes, criteria, rulings and opinions from national or international organisms, in transparency topics, can be taken into account.*”

⁹⁰ The System is composed of the INAI, local oversight bodies, the Federal Audit Office, the General Archive and the National Institute of Statistics and Geography.

taken by the INAI or the other local oversight bodies, as explained further below. A specialised body to oversee public policies on topics of transparency and data access also exists⁹¹.

Article 68 LGTAIP establishes minimum rules about data protection in public authorities, which include the need to respond to requests related to subjects' rights and guaranteeing the application of the principles of necessity and quality⁹². This provision also sets transparency rules, stating that public authorities need to provide a public document with the purposes of data processing. However, this transparency obligation does not apply to cases where the processing is based on the legal basis of performance of legal duties⁹³.

Only in case of explicit consent can the public authorities share⁹⁴ the personal data under their control⁹⁵. The consent is not needed when the information is public, when there is a legal ground for this processing, when there is a judicial order, or for reasons of national security, general health or to protect rights of a third person. The data subject's consent is also not needed when the sharing happens between public authorities or international law bodies, if this is foreseen in a treaty and if the information is used for the activities developed by those authorities. The same rules apply to requirements of access to confidential information⁹⁶.

Considering that the LGTAIP is from 2015, nowadays the data protection rules set by this law only apply if compatible with the specific laws on data protection in the public sector set by the more recent rules in the LGPDSSO, discussed in the following section. In other words, while the LGTAIP remains to be the specific law for transparency rules, the LGPDSSO – from 2017 – takes on the leading role as the specific norm for data protection in the public sector.

2.1.1.2 DATA PROTECTION IN THE PUBLIC SECTOR

The LGPDSSO is the most relevant law on data protection in the public sector, laying down its general aspects for data protection. In addition to the LGPDSSO, the INAI has published binding general guidelines on the matter⁹⁷. The LGPDSSO establishes competences for each state entity (federal, state, and district) to apply and oversee the general provisions.

Public authorities must always justify the processing of personal data controlled by them. This includes informing individuals about its purposes, which must be legal, explicit, and legitimate. All these activities must be connected to the public powers of the controlling body⁹⁸. Consequently, public authorities must provide a privacy notice with minimum information about the processing⁹⁹. In case of

⁹¹ García, 2016.

⁹² Article 68, II “[controllers are obliged] to process personal data only where such data is adequate, relevant and not excessive in relation to the purposes for which they were collected, or such processing is carried out in the exercise of the powers conferred by law”. Article 68, V “[controllers are obliged] to replace, rectify or complete, ex officio, any personal data which is inaccurate, incomplete, wholly or in part, at the time they become aware of this situation”.

⁹³ Article 68, III of the LGTAIP “The obliged subjects are responsible for the personal data under their control and must: III – make it available for individuals, from the moment of the data collection, the document that establishes the purposes of the processing, according to the legal rules that apply, except in cases in which the processing is based on the performance of legal duties.”

⁹⁴ Even though the LGTAIP mentions the selling of data, it seems that this possibility was overturned by the LGPDSSO, since this law is more specific on data protection and more recent. Article 68 paragraph 1 LGTAIP establishes that “public authorities, cannot share or commercialize personal data that are part of the information systems developed in the exercise of their public functions, unless they receive express consent, written or by a similar authentication system, of the individuals that the information relates to. This applies without prejudicing what is established by Article 120 of this law.”

⁹⁵ Article 68 of the LGTAIP.

⁹⁶ Article 120 of the LGTAIP.

⁹⁷ Lineamientos Generales de Protección de Datos Personales para el Sector Público, available at: https://www.gob.mx/cms/uploads/attachment/file/304930/lineamientos__generales_para_la_protecci_n_de_datos_personales_para_el_sector_p_blico.pdf.

⁹⁸ Article 18 of the LGPDSSO.

⁹⁹ The minimum content of privacy notices is established by Article 27 of the LGPDSSO.

the impossibility of making the notice available to the individual, the authority can apply a compensatory measure in the form of mass communication to disseminate the information¹⁰⁰.

Free, specific and informed consent¹⁰¹ is the general rule for the processing of personal data in the public sector¹⁰². Due to the imbalance of powers in the relationship between individuals and the government, having informed consent as a general rule for processing can be problematic. Therefore, the legal system provides for additional legal grounds for data processing¹⁰³ so that consent is not always mandatory. These are:

- processing is established by law, that does not contradict the LGPDSSO;
- the data processing is for a compatible purpose to the one that was set for the initial processing;
- there is a judicial order;
- processing is necessary for the recognition or defence of the subject's rights before a competent authority;
- processing is necessary for exercising a right or complying with obligations derived from a relation between data subject and the controller;
- processing is required in an emergency situation that can result in harm to individuals or their assets;
- processing is necessary for health care or sanitary reasons;
- processing relates to public information¹⁰⁴;
- processing of anonymised data; or
- when the personal data concerns a missing person, according to a specific law.

The processing of sensitive data by public authorities is prohibited unless the explicit consent of the data subject is collected or unless one of the general consent exceptions mentioned above applies¹⁰⁵. Consent is also needed for a legitimate processing of personal data for a secondary purpose, not mentioned in the privacy notice. The purpose not published must be related to the legal competences of that public authority¹⁰⁶. The exceptions for consent do not apply for secondary purposes.

Since the law establishes various exceptions for the content rule, the INAI suggests in their guidelines that public authorities clearly identify the purposes of the data processing, also stating which processing operations are based on consent and which are not¹⁰⁷.

For processing of data of minors, the principle of the best interest of the minor shall prevail and the public body must also comply with specific regulations on the topic¹⁰⁸.

Consent is also a standard legal basis to justify national or international data transfers. However, there are various exceptions to said rule. The exceptions that justify data processing without consent outlined above also apply for data transfers. In addition, there are other exceptions that also remove the need for

¹⁰⁰ Article 26 of the LGPDSSO.

¹⁰¹ In the general cases, consent can be both express or tacit, as mentioned by Article 21 of the LGPDSSO.

¹⁰² Article 20 of the LGPDSSO.

¹⁰³ Established by Article 22 of the LGPDSSO.

¹⁰⁴ The LGPDSSO establishes that the following categories are considered as sources of public information: internet websites and other electronic communications media that facilitate access to data to the public and have unrestricted access; phone books, official diaries, and publications; social communication media; and public registries.

¹⁰⁵ Article 7 of the LGPDSSO establishes “As a general rule, sensitive personal data may not be processed, unless there is the express consent of the subject or, failing that, in the cases established in Article 22 of this Law”.

¹⁰⁶ Article 18, Paragraph 1, of the LGPDSSO establishes: “the controller may process personal data for purposes other than those established in the privacy notice, as long as it has powers conferred by law and collects the subject's consent, unless it is a person reported missing, under the terms provided for in this Law and other provisions that are applicable in the matter”.

¹⁰⁷ INAI, *El ABC del aviso de privacidad, Sector Público*, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_ABC-AP-SPublico.pdf.

¹⁰⁸ Article 7, Paragraph 1, of the LGPDSSO.

consent for data transfers. Thus, in the following additional cases, a data transfer is also justified without the need of the subject's consent¹⁰⁹:

- when the transfer is foreseen in laws and international agreements or treaties;
- when the transfer is legally foreseen for criminal investigations or prosecution, as well as for law enforcement;
- when the transfer is governed with contractual or pre-contractual provisions of an instrument that the processing entity is part of;
- when the transfer is necessary for the maintenance of a judicial relationship between the controller and the subject, including for the exercise of rights or fulfilment of obligations;
- when the transfer is necessary for national security reasons.

Even though the LGPDSSO explicitly states that international or national data transfers can occur without the subject's consent in the exceptions foreseen in Articles 22, 66, and 70, outlined above, the application of these exceptions is not completely clear. For example, Article 22 establishes that consent is not necessary when the purpose of the data processing is the recognition or defence of the subject's rights before a competent authority. However, Article 70 adds an additional requirement for this scenario: the authority must request the data. Thus, it is uncertain if all the conditions for exceptions foreseen in Article 70 must be observed for data transfers.

Any data transfer involving a public authority must be formalised through contractual clauses, collaboration agreements, or any equivalent legal instrument. This obligation does not apply to national transfers that occur in order to comply with a legal provision or to exercise legal competences provided by the law¹¹⁰. The need for a legal instrument is considered fulfilled if a treaty of law already foresees the international transfer¹¹¹.

Based on the outlined provisions, international data transfers to third countries can therefore happen without the prior consent of the data subject if the above exceptions apply, meaning whenever this activity is foreseen in a Mexican law or a treaty. The same applies to international transfers carried out after a request of a foreign authority, if the purposes of the transfer are equivalent to the ones that justified the initial processing¹¹². This means that whenever the third country's purposes are compatible with the reasons why the processing of personal data started, the data transfer can happen without the subject's consent and without the need of a specific treaty or law. In any case of a data transfer to third countries, the recipient is obliged to protect the data according to Mexican law¹¹³, which needs to be verified by the controller¹¹⁴.

The INAI can publish a technical opinion on an international transfer, which can be positive or negative. It will issue such an opinion after the request of a representative. If the INAI does not publish the technical opinion within the time frame set by law, it should be understood that the authority is not favourable to the transfer¹¹⁵.

Finally, the LGPDSSO mentions the obligation of applying security measures to guarantee the protection of personal data by public authorities¹¹⁶. Adopted security measures need to be documented

¹⁰⁹ Articles 22, 66 and 70 of the LGPDSSO.

¹¹⁰ Article 66 of the LGPDSSO.

¹¹¹ Article 66, II of the LGPDSSO.

¹¹² Article 66, II of the LGPDSSO.

¹¹³ Article 68 of the LGPDSSO.

¹¹⁴ INAI, *Recomendaciones para los sujetos obligados en las comunicaciones de datos personales*, May 2022, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones-SO_Comun_DP.pdf.

¹¹⁵ INAI, *Recomendaciones para los sujetos obligados en las comunicaciones de datos personales*, May 2022, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones-SO_Comun_DP.pdf.

¹¹⁶ Article 31, LGPDSSO “*Regardless of the type of system in which the personal data are held or the type of processing carried out, the controller must establish and maintain administrative, physical and technical security measures for the protection of personal data, in order to protect them against damage, loss, alteration, destruction or unauthorised use, access or processing, as well as to guaranteeing their confidentiality, integrity and availability*”.

in a specific security document¹¹⁷, which needs to be updated whenever there are substantial changes in the data processing, affecting the risk level in terms of data security¹¹⁸. The LGDPSSO does not set any further details on these security aspects, such as minimum standards.

2.1.1.3 FURTHER PROCESSING OF PERSONAL DATA BY PUBLIC AUTHORITIES

Mexico's Constitution establishes that public authorities can only temporarily retain information for the purposes of public interest or national security, according to the relevant legal provisions obliging those authorities to record their activities¹¹⁹. This provision leaves room for a bigger societal and international scrutiny of the government's activities, since time becomes another factor of control. To implement this, Mexico has established different rules about transparency and data access (LGTAIP), which were mentioned earlier in this report, in parallel with a specific legislation about national security.

The LGTAIP establishes that every authority is responsible for classifying the level of access to the information they use. As mentioned, as a rule, personal data is considered as confidential data. Bank, fiduciary, industrial, commercial, fiscal, stock exchange and postal secrecy information are also considered confidential. As a rule, public authorities must therefore receive the consent of the data subject to allow the access to confidential information. However, the consent is not needed if the information: (i) is available in public databases; (ii) has public status set by law; (iii) is part of a judicial order for access; (iv) is needed for national security, health care or for the protection of third parties' rights; (v) is shared between public authorities or international bodies, following treaties, or (vi) when the information is needed for their activities.

In other cases, information can be classified as 'reserved', making it thereby more difficult to access or disclose. Article 113 of the LGTAIP sets that an authority can label information as reserved if: (i) it compromises the national or public security, or national defence, as long as it has a genuine purpose; (ii) can affect international relations; (iii) was delivered to Mexico as reserved or confidential information, as long as it does not affect human rights; (iv) brings risks to the economic and monetary system of the country; (v) brings risks to a person's life, security or health; (vi) obstructs the enforcement of the law or the payment of taxes; (vii) obstructs the prevention or persecution of crimes; (viii) contains information about the deliberation process of public servants, while there is no final decision; (ix) obstructs the procedures of liability of public servants, while there is no final administrative resolution; (x) affects the due process of law; (xi) affects a judicial or administrative procedure; (xii) is part of a criminal investigation under the Prosecutor's office; (xiii) is foreseen in a law or international treaty.

A ruling by the Mexican Supreme Court of Justice found that public authorities can principally disclose confidential information, for example in response to an access request, including personal data after having conducted a risk assessment. To prevent disclosure of information, public authorities must therefore demonstrate significant risks of harm to the public interest or national security to justify the classification of information as reserved or confidential¹²⁰.

¹¹⁷ Article 35, LGPDSSO, "In particular, the controller shall draw up a security document containing at least the following: I - the inventory of personal data and processing systems; II - the functions and obligations of persons processing personal data; III - risk analysis; IV - gap analysis; V - the work plan; VI - the mechanisms for monitoring and review of security measures; and VII - the general training programme".

¹¹⁸ Article 36, LGPDSSO: "The controller must update the security document whenever the following happens: I - there are substantial changes to the data processing that result in a change in the level of risk; II - as a result of a process of continuous improvement, derived from the monitoring and review of the management system; III - as a result of an improvement process to mitigate the impact of a breach of security that has occurred; and Iv - implementation of corrective and preventive actions in response to a security breach".

¹¹⁹ Article 6, A, I of the Constitution.

¹²⁰ Case n. 2018460, Thesis I.10o.A.70 A (10a), Supreme Court of Justice. November 2018.

As a rule, it is therefore prohibited to disclose information that reveals personal data, including providing access to such data¹²¹. Nevertheless, the LGTAIP also establishes that each entity is autonomously responsible for defining the classification of and the access to information. This also applies to information gathered for national security purposes¹²².

2.1.1.4 GENERAL FINDINGS OF INTERNATIONAL ORGANISATIONS

In the last 15 years, Article 19 has documented and criticised the restrictions against freedom of expression and lack of government transparency. The organisation has worked side-by-side the government in creating and implementing transparency rules to act against corruption scandals. However, the regional office of the institution has received several threats recently¹²³. In that regard, national experts have also highlighted the high number of corruption cases involving Mexican authorities¹²⁴ and the government pursuit to diminish the power provided to the INAI. For instance, there were news articles regarding the governmental attempts to discontinue the INAI¹²⁵.

Moreover, the Mexican government is increasingly relying on new surveillance technologies. Especially in touristic areas, these instruments are being adopted to allegedly bring incentives to tourism, advertising more security. These technologies are usually bought by regional governments, which may bring difficulties for the access and exploration of federal oversight mechanisms. And, even at the federal level, there are few regulations on how surveillance technologies can be acquired by Mexican public authorities¹²⁶. Such lack of regulation may lead to governmental access to personal data outside the scope of the LGPDSSO.

The national experts have highlighted that the lack of Mexican regulation on cyber surveillance allows the general use of these technologies, which can be seen in the complaints filed by reporters and human rights' advocates indicating that they have been tracked with said instruments. Even though there are different laws that establish systems of protection, the national experts have elucidated that it is not clear who is responsible for the oversight of these activities¹²⁷. Thus, the supervisory judge foreseen in the Criminal Procedures Code is the only responsible authority for setting boundaries, instead of establishing them explicitly in regulations.

2.1.2 GOVERNMENT ACCESS TO PERSONAL DATA

2.1.2.1 CRIMINAL PROCEDURE

Personal data can be accessed for the purposes of criminal procedures in Mexico when the personal data is necessary to initiate a criminal investigation or to support a criminal accusation. The personal data must be obtained in accordance with the applicable laws and regulations. Additionally, the individual whose data is being accessed must be informed of the purpose of the access.

¹²¹ Article 64 of the NSL.

¹²² Article 50 of the NSL.

¹²³ Article 19, 2022.

¹²⁴ The BTI Index was mentioned by the national experts as a way to illustrate the corruption level in Mexico, available at: <https://btiproject.org/en/reports/country-report/MEX>.

¹²⁵ Human Rights Watch (2019). *México: La transparencia y la privacidad, amenazadas*, available at: <https://www.hrw.org/es/news/2021/01/28/mexico-la-transparencia-y-la-privacidad-amenazadas>.

¹²⁶ CNDH, 2022.

¹²⁷ Interview conducted on 8 March 2023 with a representative from a public research institution. Similar remarks were made in an interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.

Different bodies have separate roles on the access to personal data by public bodies for the prevention and investigation of criminal actions. The Criminal Procedure Code (CNPP)¹²⁸ is the norm that defines the unified rules to all the Mexican jurisdictions¹²⁹ and establishes:

- the role of the police: working under the instructions of the public prosecutors' agencies, the police is responsible for the investigation of crimes;
- the role of the public prosecutors' agencies: conducting the investigation, coordinating the police forces and the experts, deciding about moving forward with a prosecution and ordering relevant actions to guarantee enough evidence for a conviction or acquittal.

As a rule, following the LGPDSSO, the data subject should be notified about any processing of their personal data, including for law enforcement activities. However, to enable some investigation activities, the CNPP establishes cases in which the subject will not be notified in advance about the access to their personal data. There are therefore two investigatory measures, that can take place without previous notification of the subject: (i) interception of private communications and (ii) access to geolocation data. Law enforcement agencies can thus access private communication or geolocation data for investigation purposes, as further explained below. While the data subject is not notified in these scenarios, a Court will be involved to guarantee the proportionality of the measures.

Prosecution authorities – or their delegates – can request a court¹³⁰ to authorise the intervention on private communications¹³¹, justifying the object and need of said activity. A judicial order is also required in cases of extraction of information¹³² and to extend the intervention to another person¹³³. The intervention can last up to six months. This period cannot be prolonged, except when the prosecution officer can prove that there are new justifying elements¹³⁴. An intervention cannot happen when the request is related to electoral, fiscal, mercantile, civil, labour, or administrative topics. Another limit is the communication between the arrested and his/her lawyer¹³⁵.

The public servants authorised to execute the activity are responsible for complying with the terms of the judicial order¹³⁶, and all persons involved in the measure must maintain the secrecy¹³⁷. The police or the experts involved in the intervention activity must register the information guaranteeing its quality, so that it can be used as evidence in the procedure¹³⁸. Not following the rules of the surveillance procedure leads to the inadmissibility of the evidence and can lead to administrative or criminal liability of the responsible officer¹³⁹. The appropriate judicial body will order the destruction of unnecessary or unlawful data. The exclusion of information will also happen when the procedure is dismissed or definitively archived, or with the acquittal of the investigated person¹⁴⁰.

¹²⁸ Código Nacional de Procedimientos Penales, de 5 de marzo de 2014.

¹²⁹ The CNPP was the first unified Code about criminal procedures. Before the norm was put into force, there were 33 different codes about this matter in Mexico – one for each jurisdiction.

¹³⁰ Suitable federal judge expert in control (*Juez federal de control competente*).

¹³¹ Private communications are defined as “*the whole system of communication or the applications products of technological evolution, that allow the exchange of data, information, audio, video, messages, and also the electronic file that record, retain the content of the conversations or that register the data that identify the communication, which can be presented in real time*

¹³² Extraction of information is defined as “*the collection of private communications, data that allows the identification of the communication. Also, the information, documents, text files, audios, images or videos retained in any device, accessory, electronic instrument, informatic equipment, retaining devices and everything that may contain information, including the ones storage in platforms or in remote data centres.*” (Article 291 of the CNPP).

¹³³ Article 296 of the CNPP.

¹³⁴ Article 292 of the CNPP.

¹³⁵ Article 294 of the CNPP.

¹³⁶ Article 291 of the CNPP.

¹³⁷ Article 302 of the CNPP.

¹³⁸ Articles 297 and 298 of the CNPP.

¹³⁹ Article 299 of the CNPP.

¹⁴⁰ Article 300 of the CNPP. When there is a temporary archive of the procedure, the information can be retained until the offence is prescribed.

A similar procedure must be followed for accessing geolocation data or sharing the retained data by the telecommunication companies¹⁴¹. The prosecutors' agencies will request the suitable court to authorise the sharing of said communication, explaining the reasons and purposes of the measure¹⁴². The Code does not mention a specific time limitation of this sharing.

In cases of danger of maintaining the physical integrity or the life of a person, or when the victim of the crime is in danger, or in cases related to abduction of a person, the prosecutor officer will directly command the sharing of the geolocation data or the retained data. In these circumstances, the prosecutor agent or the capable person works under personal liability. The authority must notify the responsible court about the measure within 48 hours, so that the measure can be confirmed – partially or totally. The court can also not ratify the measure, making the information collected inutile for the criminal procedure.

Similarly, the prosecutor or the delegated agent can request the telecommunication companies to retain data contained in networks, systems, or computer equipment. This measure starts immediately after the request or the judicial order¹⁴³ and can last up to 90 days¹⁴⁴.

Competent courts provide oversight for the activities described above.

For access to personal data in communications, the law is not clear on whether data subjects are at any point notified about these measures. Whenever data subjects become a part of the criminal procedure, they can get access to information about surveillance matters. However, if they never formally become a part of the procedure (e.g. if they are never charged), they may never be notified about the access to their communications. This is because there is no obligation of prior notification, as explained above, and it is not clear in the CNPP whether there needs to be a mandatory notification after the execution of the activity¹⁴⁵. In the interviews with national experts, one expert clarified that “recently, there was a big reform on the telecommunication field. Legal obligations were set on telecommunication companies to record and have available all the data related to the services they provide. A platform was created to process all the requests of access to these databases. Nowadays, telecommunication companies have one main obligation that is to maintain the data and to use this platform to be in contact with the authorities. The new systems also brought obligations to the public authorities to always use this platform for requesting information for telecommunication companies. Even though there were relevant changes, the transparency obligations are still there. What has changed is the way used to comply with the obligations. Currently, telecommunication companies must use the mentioned platform for access in the telecommunications field”¹⁴⁶. The national experts also explained that, “there is no transparency report that has been able to provide information about how often interceptions occur”¹⁴⁷.

¹⁴¹ Telecommunication companies shall be understood as any company authorised or operator of telecommunication, and access providers, established by Article 303 of the CNPP.

¹⁴² Article 303 of the CNPP.

¹⁴³ This measure follows the same procedure as what is set by the access to geolocation data and its exception in case of imminent danger.

¹⁴⁴ Article 303 of the CNPP.

¹⁴⁵ This was pointed out to the authors in an interview on 2 March 2023, with representatives from a leading Mexican law firm. The experts noted: “There are no rules about the need to notify the subject. For investigation purposes, the individuals are not notified that they are being targeted with a surveillance mechanisms such as the interception of private communications. Thus, even if there is a mistake in the processed data, the subject cannot exercise rights since they are not aware that the information is being processed in cases of national security or law enforcement. A different situation exists when the information is directly obtained by an individual. In such cases, the individuals may exercise their rights to access, rectification, cancellation or objection (ARCO) under the data protection laws.”

¹⁴⁶ Interview conducted on 3 March 2023 with a representative from a leading Mexican law firm.

¹⁴⁷ Interview conducted on 2 March with a representative from a leading Mexican law firm. This was further confirmed in an interview conducted on 8 March 2023 with a representative from a public research institution.

2.1.2.2 INTELLIGENCE ACTIVITIES AND NATIONAL SECURITY

All actions and authorities for the purpose of preserving the national security in Mexico must comply with the National Security Law (NSL)¹⁴⁸. The legal rules also establish how the different entities, local and federal, can collaborate for this purpose. The law establishes that personal data processed by national security authorities in Mexico in order to establish or prevent a national security threat is confidential governmental information¹⁴⁹. Confidential information can only be accessed in a limited manner by individuals.

Throughout the development of intelligence activities¹⁵⁰, the authorised public authorities may use any means of collection of information, if the individual freedoms and human rights are observed¹⁵¹. Additionally, public servants involved in activities related to national security must observe the following principles even though they are not defined in the NSL¹⁵²:

- the legality principle;
- responsibility;
- respect for fundamental rights;
- confidentiality
- loyalty;
- transparency;
- efficiency; and
- coordination and cooperation.

Intelligence activities shall always observe the purposes of national security while preserving the democratic State¹⁵³. As illustrated by a national expert, “*national security is a legal reason for mitigating fundamental rights. However, this mitigation is limited, the principles of legality and proportionality must be observed. The analysis of possibility of mitigation is evaluated case by case*”¹⁵⁴.

Intelligence agencies can perform interception of communications¹⁵⁵. A judicial warrant is needed for said surveillance measure¹⁵⁶ and this will only happen in cases of imminent threat to national security¹⁵⁷. To oversee this procedure, the competent Court can request information about the measure at any moment and will also determine for how long the surveillance can take place¹⁵⁸. The information gathered through this procedure cannot be used as evidence in administrative or judicial procedures. Intervention of private communication for law enforcement must comply with the CNPP¹⁵⁹.

National security activities are overseen by the legislative power. A bicameral commission¹⁶⁰ is responsible for conducting the oversight. The legal provisions are generic and include the possibility to

¹⁴⁸ Ley de Seguridad Nacional (NSL).

¹⁴⁹ Articles 6, V and 63 of the NSL.

¹⁵⁰ Intelligence is defined by the NSL as “*any knowledge obtained by the collection, processing, dissemination and exploration of information, for decision-making in matter of national security*” (Article 29).

¹⁵¹ Articles 31 and 61 of the NSL.

¹⁵² Article 61 of the NSL.

¹⁵³ Article 3 of the NSL.

¹⁵⁴ Interview conducted on 8 March 2023 with a representative from a public research institution.

¹⁵⁵ According to Article 39 of the NSL, the interception can apply to “*private communications and emissions, made through any transmission mean, already known or to be known, including images recordings*”.

¹⁵⁶ Even in urgent cases, as established by Article 49 of the NSL “*In exceptional cases, when compliance with the procedure established in the Section II of this Chapter compromises the success of an investigation and there are indications that a threat to National Security may be consummated, the judge, due to urgency, may authorise immediately [the interception] as required*”.

¹⁵⁷ Articles 34 and 35 of the NSL.

¹⁵⁸ The intervention can last up to 180 days. This timeline can be renewed for the same period by another judicial order, as long as there are reasons for that (Articles 43 and 44 of the NSL).

¹⁵⁹ Article 36 of the NSL.

¹⁶⁰ With three Senators and three deputies.

request information from the authorities involved in the national security activities and evaluate reports about such actions¹⁶¹. However, such a report can be broad and there are no specific legal requirements about the content of these documents¹⁶². Such dossiers will also omit any information that affects national security and activities for such purposes or the privacy of individuals. This is because no registry shared with the oversight body should contain confidential information¹⁶³.

The NSL also establishes that the oversight and the execution¹⁶⁴ of interventions for national security purposes are the responsibilities of the Centre of Investigation and National Security¹⁶⁵ (*Centro de Investigación y Seguridad Nacional - CISEN*, in the Spanish acronym). In 2018, the CISEN was substituted by the National Centre of Intelligence (*Centro Nacional de Inteligencia - CNI*, in the Spanish acronym).

The CNI is an autonomous and decentralised body¹⁶⁶. Thus, there are legal provisions about the internal oversight of national securities activities. In cases not addressed by the NSL, judiciary oversight shall be observed, and the Federal Code of Civil Procedures and the Organic Law of the Judiciary Power of the Federation will prevail and must be followed¹⁶⁷. In gap scenarios involving the principle of transparency, the General Law for Transparency and Access to Public Data shall be considered, and, in these exceptions the INAI can act in overseeing the activities.

Following the legal obligations related to personal data, the CNI has published its privacy notice¹⁶⁸. This document, however, only addresses the personal data processed to control the access of the building. Together with the privacy notice, the CNI published a guide on how to exercise the ARCO rights before the CNI¹⁶⁹. On this opportunity, the CNI clarified that if a legal provision blocks these rights, it will not respond to the requests. It is important to note that the responses to said requests can be reviewed by the INAI, since the CNI is a federal body. The data protection documents, however, reaffirm that data processing for national purposes is an exception to the rules set out by the LGPDSSO and even to the constitutional rights to data protection. Thus, even though the LGPDSSO is a more recent law, it does not seem that it affects the provisions of the NSL. Academic research has shown that citizens' requests to national security agencies for access to data tend not to be fully responded to¹⁷⁰.

2.1.2.3 OVERSIGHT MECHANISMS

This section describes the oversight and redress mechanisms for the public and private sector excluding national security activities. The oversight and redress mechanisms for national security activities were described at the end of the previous section 2.1.2.2 on intelligence activities.

¹⁶¹ Article 57 of the NSL.

¹⁶² Article 58 of the NSL establishes that “In the months in which the regular sessions of the Congress begin, the Technical Secretary of Council [of National Security] must render to the Bicameral Commission a general report of the activities carried out in the immediately preceding semester. The Bicameral Commission may summon the Technical Secretary to explain the content of the report.”

¹⁶³ Article 59 of the NSL.

¹⁶⁴ One of the attributions of the Centre is to “operate intelligence tasks as part of the national security system that contribute to preserving the integrity, stability, and permanence of the Mexican State, to support governance and to strengthen the rule of law” (Article 19, I NSL).

¹⁶⁵ Article 41, NSL.

¹⁶⁶ Article 18, NSL.

¹⁶⁷ Article 8, III, NSL.

¹⁶⁸ CNI, *Aviso de Privacidad Integral*, available at: <http://www.cni.gob.mx/transparencia/docs/Aviso-Privacidad-Integral.pdf>.

¹⁶⁹ CNI, *Guía para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales*, available at: <http://www.cni.gob.mx/transparencia/docs/Guia-ARCO.pdf>.

¹⁷⁰ López, L. C. J., ‘Seguridad nacntional, inteligencia militar y acceso a la información en México’, *URVIO Revista Latinoamericana de Estudios de Seguridad*, no. 21, 2017, available at: http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-42992017000100140&script=sci_arttext.

For the public sectors, different actors are tasked with providing oversight. Considering the system set by the LGPDSSO and the LGTAIP, each federal entity must have a competent authority to oversee data protection, data access and the transparency rules. The INAI is the federal authority and each state and the Federal District come with a local authority.

Each local oversight authority¹⁷¹ is the first instance for oversight over activities of public authorities. Thus, if a municipal or state public authority has an action challenged by an individual, this matter should be taken first to the local oversight authority. In the same sense, if the challenged action is made by a federal public authority, the INAI is the body responsible for oversight. However, the INAI can also be considered as a second instance, since it is an autonomous body that oversees the activities of the regional authorities. The oversight activities developed by the INAI can start either *ex officio* or be based on a complaint¹⁷².

In any case, decisions by the oversight authorities can be challenged judicially. Federal judicial courts can overturn the delivered decisions of the specialised bodies, acting as the last instance of the oversight system. Also, the Supreme Court can be called upon to decide in disputes, especially considering that data protection is a fundamental constitutional right.

For the private sector, the INAI's role of overseeing the enforcement of the LFPDSSPP may occur by the initiative of the own authority or by a petition of a party. In case a private party does not observe the legal provisions¹⁷³, the INAI may initiate a procedure to apply sanctions, especially fines. Provoking a data breach for profit is considered a crime. Processing personal data accessed after an error of the data subject or of a third party is also considered to be a crime¹⁷⁴.

2.1.3 DATA SUBJECT RIGHTS

2.1.3.1 AVAILABLE RIGHTS AND THEIR SCOPE OF APPLICATION

The constitutional rights are reinforced by the specific Mexican laws on data protection (LFPDSSPP and LGPDSSO). Considering the constitutional aspects of data protection, both laws apply to any person, regardless of their nationality, if they follow the respective procedure.

Article 22 of the LFPDSSPP stipulates that any person – or their legal representative – may exercise, at any time, the right to access, correction, objection, and opposition (*derechos ARCO*). Limits exist for the exercise of those rights. Correction may only occur when the data is incorrect or incomplete¹⁷⁵. The right to objection is limited, since the controller is not obliged to exclude the information when there is a legal exception, which includes following a legal obligation¹⁷⁶ and to act in the public interest¹⁷⁷. The right to access data is also related to the transparency rules set by the LGTAIP. This law establishes that the request to data access is free of charge, which can change in cases of requests of reproduction or delivery of the data¹⁷⁸. Requests can receive a positive or negative response by an authority. These responses, can, as explained above in section 2.1.2.1, be reviewed by the competent authorities via revision claims.

¹⁷¹ Considering that each Mexican jurisdiction must have a specific and local authority to oversee the activities of transparency and data protection.

¹⁷² INAI, *Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf.

¹⁷³ Article 59 of the LGPDSSPP.

¹⁷⁴ Articles 67 and 68 of the LGPDSSPP.

¹⁷⁵ Article 25 of the LGPDSSPP.

¹⁷⁶ Article 26, II of the LGPDSSPP.

¹⁷⁷ Article 26, V of the LGPDSSPP.

¹⁷⁸ Article 17 of the LGTAIP.

Requests to exercise data subject's rights may be denied in cases where (i) the request was sent by someone other than the data subject who is not credited as a legal representative; (ii) the personal data are not part of the databases of the company¹⁷⁹; (iii) the rights of a third party are affected; (iv) the request has already been addressed; or (v) there is a decision of a competent authority limiting said rights¹⁸⁰.

The controller must provide an answer to the data subject within 20 days and in case of complying with the request, the controller must solve the question in the following 15 days. However, when private companies are responsible for the processing of personal data, some internationally recognised subjects' rights do not apply, since there are no provisions regarding the right to be forgotten, the right to restrict processing and the right to data portability.

The INAI is responsible for assuring the compliance of private parties with the LFPDSSPP, which includes the oversight of auto-regulatory practices – codes of good practices, that should facilitate the exercise of rights – alongside sectorial authorities¹⁸¹.

Similar provisions apply to the public sector¹⁸². However, some differences apply. For instance, the complaints must be targeted to the competent authority, which include regional oversight bodies. As explained in section 2.1.2.2 above, the system for data protection in the public sector relies on the actions of different authorities. The INAI is responsible for the oversight of data processing activities of federal bodies, including bodies working for national security purposes. State and municipal public authorities have their processing activities overseen by local authorities. Thus, in cases where the data subject does not agree with the response to their requests, the individual can first complain to the local authority.

Regarding the right to objection, the data subject can request the exclusion of their personal data from archives, registries, and other systems¹⁸³, explaining the reasons behind the request¹⁸⁴. However, there are limitations to this exercise. For instance, telecommunication companies must keep information for 90 days. According to this legal provision, the data subject cannot object to this retention of data, since the processing is necessary for a legal obligation.

A data subject can also oppose or cancel any processing that may cause any harm to him or her. This provision includes automated processing that may affect the interest, rights, and freedoms of data subjects, if there is no human participation and the purpose of this activity is profiling the subject. A data subject must identify the risks or harms of the processing¹⁸⁵.

The right to portability applies to data controlled by public authorities. Upon request, the public authority shall provide a copy of the personal data controlled by the body. The information must be in an interoperable electronic format¹⁸⁶.

Beyond the possibilities set by the LFPDSSPP, public authorities may also reject requests under different circumstances¹⁸⁷. Thus, public authorities can deny requests that might harm judicial or administrative activities or that are directed to a public body that is not competent. Data processing can continue when necessary to protect legitimate interests or to comply with legal obligations of the subject,

¹⁷⁹ In this case, the request should be directed to the controller of the personal data.

¹⁸⁰ Article 34 of the LGPDSSPP.

¹⁸¹ Articles 43 and 44 of the LGPDSSPP.

¹⁸² Third tile – Data subjects rights and exercise – of the LGPDSSO.

¹⁸³ Article 46 of the LGPDSSO.

¹⁸⁴ Article 52, Paragraph 5 of the LGPDSSO.

¹⁸⁵ Article 52, Paragraph 6 of the LGPDSSO.

¹⁸⁶ Article 57 of the LGPDSSO.

¹⁸⁷ Article 55 of the LGPDSSO.

and when the maintenance of the Mexican state relies on this activity. The requests can also be denied when the data is related to the financial oversight duties of the subject¹⁸⁸.

After receiving the request, the public authority has up to 20 days to respond. This period can be amplified up to 10 more days if the data subject is notified. In case of a positive response to the request, the public body also has 15 days to apply the desired measure¹⁸⁹.

When the data subject is not satisfied by the solutions provided by the regional oversight body, they can ask for review at the INAI. However, the Mexican Supreme Court of Justice ruled that constitutional matters cannot be solved by the INAI when the competence is held by the higher court¹⁹⁰. Another decision by the Mexican Supreme Court established that when judicial bodies are deciding about matters related to the INAI's competences, the courts do not have to limit their analysis to what was already established by the INAI¹⁹¹.

Data breaches in the public sector require actions of the authorities. The controller must present an action plan to guarantee the protection of the data, analysing the plausible causes of the vulnerability. The public authority must immediately notify the data subject. Whenever the violation can substantively affect rights, the INAI should also be notified¹⁹².

As highlighted by lawyers, the systems set up for the public and private sector are very similar. However, data subjects have more difficulties in enforcing their rights under public authorities. A national expert believes the opposite applies, especially considering that the majority of data protection procedures are set in big Mexican cities, where the most structured public entities are also established.

Finally, it is essential to remember that the ARCO rights are fundamental rights, constitutionally protected¹⁹³. As a result, they should be complied with in every data-processing activity, regardless of the nationality of the subject. Observing the purposes of the processing, the ARCO rights can only be mitigated when the measure is proportional and necessary. In specific cases, special legislation should also be taken into account. When data is processed for law enforcement purposes, the National Criminal Procedures Code applies. In the framework of national security activities, the NSL applies. However, specialists confirmed that there are no specific legal provisions about the right to be informed of being the target of surveillance measures once they are concluded, as also detailed in section 2.1.3.1. According to the interviewed national experts, subjects "*are not aware that their information is being processed in cases of national security or law enforcement access*"¹⁹⁴.

2.1.3.2 REDRESS MECHANISMS

In the private sector, once a data subject receives a response to a request to exercise data protection rights from a private controller or the period of response is over, the individual has 15 days to submit a complaint to INAI¹⁹⁵. After receiving the complaint, the INAI receives and gathers evidence to then resolve the request within 50 days - that can be extended to 100 days¹⁹⁶ - which may include

¹⁸⁸ See further Articles 52 and 55 of the LGPDSSO. The INAI has not published any specific guideline further clarifying when such situations occur.

¹⁸⁹ Article 51 of the LGPDSSO.

¹⁹⁰ Case 2024641 of the Supreme Court of Justice of May of 2022, Thesis 2a./J. 23.2022 (11a)..

¹⁹¹ Case n. 2011608 of the Supreme Court of Justice of May of 2016, Thesis 2a. XIX/2016 (10a)...

¹⁹² Article 40 of the LGPDSSO: "*The controller shall promptly inform the data subject, and as applicable, the INAI and the local oversight bodies, of any breaches that significantly affect rights, as soon as it is confirmed that the breach has occurred and that the controller has begun to take actions aimed at triggering an exhaustive review process of the magnitude of the breach, so that the affected data subjects may take the corresponding measures to defend their rights*".

¹⁹³ Article 16, Constitution.

¹⁹⁴ Interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.

¹⁹⁵ Article 45 of the LGPDSSPP.

¹⁹⁶ Article 47 of the LGPDSSPP.

reconciliation between the parties. In case of a positive outcome for the data subject, the controller has 10 days to comply with the request. When another competent court is following a procedure that might modify or revoke INAI's decision, the national authority may conclude that the complaint is inadmissible¹⁹⁷. Following the INAI's decision of the complaint, the parties may request the annulment of the decision to the Federal Court of Fiscal and Administrative Justice (*Tribunal Federal de Justicia Fiscal y Administrativa*)¹⁹⁸.

The national experts interviewed noted that the judicial courts tend not to take into account the guidelines issued by the INAI. This has to do with the fact that Supreme Court has determined that these documents are non-binding¹⁹⁹.

Besides the complaints related to the exercise of data protection rights, data subjects may also ask for compensation when they consider that there was any harm to their goods or rights, according to specific norms²⁰⁰, including the civil legislation of liability.

There are different options for redress against actions by public authorities as elaborated upon by one of the interviewed experts²⁰¹. As a rule, when individuals have a complaint about the compliance of any action with data protection rules, they should address it first to the public authority, as the author of the activity, first. If the individuals concerned still disagree with the response - or there is a lack thereof, they can then lodge a complaint to the oversight authorities. In case of federal bodies this will be directed to the INAI. For activities of municipal or state authorities, the complaint should be directed to the local oversight authorities. After a resolution of a complaint by a local authority, the dispute can still be forwarded to the INAI as a second instance. These processes follow the general administrative procedural rules. Where the non-compliance with data protection rules also constitutes a crime, the individual or the Prosecutor's Office in charge can go directly to the court system, following the criminal procedure rules. As reported by one of the interviewed experts, in one instance, the INAI has brought a data protection incident that was a potential criminal act to the attention of the competent authority²⁰². However, in this case, as explained by the interviewed national expert, this happened based on the general duty of every person to report crimes, not because of any formal cooperation²⁰³. The INAI has no formal powers to bring cases to court. Judicial bodies can also be involved in disputes regarding data protection when authorities use the information beyond judicial orders or when there is an abusive request to access confidential information.

2.1.4 OVERVIEW OF RELEVANT LEGISLATION

Public authority activity	Laws applied	Oversight	Redress mechanisms
National Security	National Security Law	Legislative bodies	N/A
Law enforcement purposes	Criminal Procedures Code LGPDSSO	Judiciary INAI	Judiciary
General rules of data access	LGPDSSO LGPDSSP Local legislations	INAI	INAI Judiciary

¹⁹⁷ Article 52, III of the LGPDSSPP.

¹⁹⁸ Article 56 of the LGPDSSPP.

¹⁹⁹ Interview conducted on 8 March 2023 with a representative from a public research institution. A similar remark was made in an interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.

²⁰⁰ Article 58 of the LGPDSSPP.

²⁰¹ Interview conducted on 8 March 2023 with a representative from a public research institution.

²⁰² Interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.

²⁰³ Ibid.

2.2 TÜRKİYE

2.2.1 RULE OF LAW, RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

2.2.1.1 CONTEXT AND CONSTITUTIONAL LAW

Türkiye is a constitutional republic with a presidential representative democracy. Similar to most EU Member States, the legal system in Türkiye is based on civil law with codified laws²⁰⁴. According to Article 2 of the Turkish Constitution, the Republic of Türkiye is a “*democratic, secular and social state governed by rule of law*”²⁰⁵. Following a referendum held on 16 April 2017, fundamental changes to the governing structure were introduced by exchanging the long-standing parliamentary system with a *sui generis* quasi-presidential system. Hence, the Constitution underwent considerable amendments with the new system becoming effective as of 9 July 2018. In principle, the Constitution provides a separation of powers (i.e., legislative, executive and judicial) between the parliament²⁰⁶, the president (the head of state and head of government)²⁰⁷, and the judiciary²⁰⁸.

Türkiye is a founding member of the United Nations and has been a member of the Council of Europe (CoE) since 13 April 1950. Since December 1999, Türkiye has been an EU candidate country and accession negotiations started in 2005 but have not advanced recently. Moreover, Türkiye and the EU have been expanding their economic and trade relations since 1963, through the Ankara Association Agreement, and a Customs Union which was established in 1995.

In terms of international obligations, Türkiye signed and ratified the European Convention of Human Rights (ECHR) in 1954, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as well as the UN’s International Covenant on Civil and Political Rights. However, the updated version of the Convention 108 on protection of individuals with regard to the Processing of Personal Data (Convention 108+) is yet to be signed and ratified²⁰⁹. By signing and ratifying the above documents, Türkiye commits to the protection of human rights, including the right to privacy and data protection.

Since December 2022, Türkiye has also been party to the Organisation for Economic Co-operation and Development (OECD) intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes²¹⁰.

²⁰⁴ Case law is also taken into consideration for the interpretation of laws.

²⁰⁵ Excerpted from the official English translation of the Constitution of the Republic of Türkiye provided by Grand National Assembly of Türkiye (GNAT), May 2019, available at:

https://www5.tbmm.gov.tr/yayinlar/2021/TC_Anayasasi_ve_TBMM_Ic_Tuzugu_Ingilizce.pdf.

²⁰⁶ Article 7 of the Constitution of Türkiye: “*Legislative power is vested in the Grand National Assembly of Türkiye on behalf of Nation. This power shall not be delegated.*”

²⁰⁷ Article 8 of the Constitution of Türkiye: “*Executive power and function shall be exercised and carried out by the President of the Republic in conformity with the Constitution and laws.*”

²⁰⁸ See Chapter 3 “*Judicial Power*”, Articles 138-160 of the Constitution of Türkiye.

²⁰⁹ It is important to highlight that an international agreement duly approved and enacted by the legislature is also deemed to be part of the legal system and Article 90(5) of the Constitution privileges international agreements related to fundamental rights and stipulates that “*International agreements duly put into effect have the force of law. In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail.*”, see Article 90(5) of the Constitution.

²¹⁰ OECD, *Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access*, available at: <https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm#>.

The Constitution of Türkiye²¹¹ includes protection for several basic human rights and freedoms such as the right to privacy²¹², freedom of communication²¹³, and freedom of expression²¹⁴. The Constitution also introduces certain guarantees and conditions for the limitations of those rights²¹⁵. In particular, Article 13 stipulates that fundamental rights and liberties may be limited only by law²¹⁶ and for the reasons specified in the relevant Articles of the Constitution, without prejudicing their essence. These restrictions must not be contrary to requirements of the democratic order of society and the secular republic, as well as the proportionality principle. Additionally, Article 16 of the Constitution of Türkiye stipulates that “*The fundamental rights and freedoms in respect to aliens may be restricted by law compatible with international law.*” Article 20 of the Constitution of Türkiye guarantees privacy and data protection rights to everyone and further introduces restrictions to the state’s interference with the processing and recording of such data in line with the ECHR²¹⁷. Furthermore, this provision also entitles individuals to the right to be informed, the right of access and the right to request correction and deletion of their personal data.

2.2.1.2 THE HUMAN RIGHTS SITUATION IN TÜRKİYE

There are serious deficiencies in the protection of fundamental rights and functioning of Türkiye’s democratic institutions. Türkiye had the most registered violations of human rights of the ECHR, with a total of 3 900 judgments of the European Court of Human Rights (ECtHR) in the period 1959-2022²¹⁸. A report of the EU highlighted the fact that although human and fundamental rights are enshrined in the Turkish Constitution and legislations, a “serious backsliding” in terms of the rule of law and human rights is the reality²¹⁹. As of December 2022, 20 100 applications against Türkiye were pending before the ECtHR²²⁰. Türkiye has been found to have violated the right to respect for private and family life 140 times by the ECtHR during the period 1959-2022. In light of this, the CoE condemned the human rights situation in Türkiye and repeatedly criticised it for not complying with the ECHR. In February 2022, the CoE agreed on developing further restrictive measures in response to the serious violations of human rights in Türkiye and non-compliance with ECtHR decisions²²¹.

²¹¹ Articles 17 to 40 of the Constitution of Türkiye.

²¹² Article 20 of the Constitution of Türkiye.

²¹³ Article 22 of the Constitution of Türkiye.

²¹⁴ Article 26 of the Constitution of Türkiye.

²¹⁵ Articles 13, 14 and 15 of the Constitution of Türkiye introduce safeguards and conditions to the limitations of human rights.

²¹⁶ It is important to underline that the concept of law in this sense corresponds to an act that is formally adopted by the Grand National Assembly of Türkiye by excluding executive or secondary legal instruments to restrict fundamental rights. Thus, the Constitution take stricter approach to the restriction of fundamental rights.

²¹⁷ Following the amendments of 2010, Article 20 of the Constitution of Türkiye: “*Everyone has the right to demand respect for his/her private and family life. Privacy of private and family life shall not be violated*”.

²¹⁸ As of December 2022, Türkiye has been found to violate the right to life (Article 2 ECHR) 143 times, and lack of effective investigation (Article 2 ECHR) 225 times, the right to inhumane or degrading treatment (Article 3 ECHR) 348 times, and lack of effective investigation to (Article 3 ECHR) 229 times, the right to liberty and security (Article 5 ECHR) 843 times, the right to a fair trial (Article 6 ECHR) 991 times, right to respect for private and family life (Article 8 ECHR) 140 times, freedom of expression (Article 10 ECHR) 426 times and the right to an effective remedy (Article 13 ECHR) 283 times. Other important rights are for example freedom of thought, conscience and religion (Article 9 ECHR): 13 times, freedom of assembly and association (Article 11 ECHR): 117 times, prohibition of discrimination (Article 14 ECHR): 20 times. All statistics are from the Council of Europe, viewed 12 February 2023, available at:

https://www.echr.coe.int/Documents/Stats_violation_1959_2022_ENG.pdf.

²¹⁹ EU Commission, *Türkiye 2022 Report*, available at: <https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCRkiye%20Report%202022.pdf>.

²²⁰CoE, *European Court of Human Rights, Annual Report 2022*, p. 142, available at: https://www.echr.coe.int/Documents/Annual_report_2022_ENG.pdf.

²²¹ Human Rights Watch, *Council of Europe Sanctions Turkey*, available at: <https://www.hrw.org/news/2021/12/03/council-europe-sanctions-T%C3%BCrkiye>. See also the decision taken by CoE, see Concil of Europe, *Interim Resolution on Execution of the judgment of the European Court of Human Rights Kavala against Turkey*, available at: <https://rm.coe.int/0900001680a4b3d4>.

Similarly, the EU raised several concerns regarding the deterioration of the rule of law and fundamental rights²²² in Türkiye, which have brought the accession negotiations almost to a standstill²²³. One of the concerns is the systemic lack of independence of the judiciary and the undue pressure on judges and prosecutors by the government. As stated in the most recent progress report of the EU on Türkiye the serious backsliding observed since 2016 as a consequence of the failed coup attempt is continuing. The report also highlights that despite the lifting of the state of emergency in July 2018, presidential decrees issued during the state of emergency following the failed coup attempt continue to have severe implications on fundamental rights²²⁴. In this regard, the United Nations Human Rights Council (the HRC) and the CoE Venice Commission called Türkiye to limit the duration and the scope of far-reaching emergency decrees and to introduce provisions for adequate judicial review²²⁵.

NGOs such as Amnesty International and Human Rights Watch (HRW)²²⁶ also reported that despite the newly proposed human rights' action plans and judicial reform packages, serious flaws in the judicial system persists. As a consequence, opposition politicians, journalists, human rights defenders, and others have been subjected to illegitimate investigations, prosecutions, and convictions²²⁷. With regard to counter-terrorism and human rights, the HRW notes that the counter-terrorism law in Türkiye is rather broad and vague which allows it to be used for politically motivated prosecutions of dissidents in particular for alleged "membership of a terrorist organisation"²²⁸,²²⁹.

When it comes to organisations specialised in privacy and data protection rights, Privacy International has raised concerns about the lack of safeguards against public and private surveillance in Türkiye, which were also observed in relation to the investigations initiated after the failed coup attempt²³⁰ and COVID-19 tracking²³¹.

In Türkiye, there are a variety of data retention requirements imposed upon private companies. For instance, the mandatory retention of traffic data is imposed upon telecommunication service providers

²²² For example, it is noted that Türkiye withdrew from the CoE Istanbul Convention-on preventing and combating violence against women and domestic violence, draw severe criticisms from several NGOs and international organisations. See EU Commission, *Türkiye 2022 Report*, p. 141, available at: <https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrk%20Report%202022.pdf>.

²²³ EU Commission, *Türkiye 2022 Report*, p. 5, available at: <https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrk%20Report%202022.pdf>.

²²⁴ See EU Commission, *Türkiye 2022 Report*, p. 5, p. 4: "Some legal provisions granting government officials extraordinary powers and retaining several of the restrictive elements of the state of emergency remained integrated into law, which continued to have a significant impact on democracy and fundamental rights." also echoed in the report of 2020 and 2021. See also "Under the state of emergency, Turkey derogated from its obligations under the European Convention on Human Rights and the International Covenant on Civil and Political Rights. When the state of emergency ended, all derogations were revoked but Parliament has permanently adopted most of the 36 statutory decrees issued under the state of emergency.", available at: <https://www.gov.uk/government/publications/turkey-country-policy-and-information-notes/country-policy-and-information-note-gulenist-movement-turkey-february-2022-accessible-version>.

²²⁵ European Commission for Democracy Through Law (Venice Commission), *Draft Opinion on the Provisions of the Emergency Decree Law N° 674 Of 1 September 2016 Which Concern the Exercise of Local Democracy In Türkiye*, p. 21, available at: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2017\)021-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2017)021-e).

²²⁶ Human Rights Watch (2022), *Word Report Türkiye Chapter*, available at: <https://www.hrw.org/world-report/2022/country-chapters/T%C3%BCrk%20Report>.

²²⁷ Amnesty International, *Report 2021/2022*, p. 371.

²²⁸ In the similar vein, the United Nations High Commissioner for Human Rights (OHCHR) also raised concerns over the enjoyment of the right to fair trial and access to justice while a pattern of persecution of lawyers representing individuals accused of terrorism is observed. See The United Nations Human Rights Council Working Group on the Universal Periodic Review, *Compilation on Türkiye Report of the Office of the United Nations High Commissioner for Human Rights*, , 20–31 January 2020, p. 5.

²²⁹ Ibid, p. 6.

²³⁰ Statewatch, *Algorithmic persecution in Turkey's post-coup crackdown: The FETÖ-Meter system*, 25 November 2021.

²³¹ Privacy International (2015), *The Right to Privacy in Türkiye*, available at: https://privacyinternational.org/sites/default/files/2017-12/UPR_T%C3%BCrk%20_0.pdf, and Privacy International search on Türkiye, available at: <https://privacyinternational.org/examples/3728/T%C3%BCrk%20-prepares-comprehensive-quarantine-surveillance>.

by the Authorisation Regulation on the Electronic Communication Sector²³². This Regulation aims to determine the procedures and principles for authorisation regarding electronic communication services, networks and infrastructures. Article 16 of the Regulation imposes a number of requirements on electronic communication service providers. The mandatory retention of traffic data is one of these responsibilities under Article 16(1)(f). According to this provision, access providers or the operators providing the telephone service are obliged to retain the following data for two years: the IP address of the parties, the port range, the start and end time of the service provided, the type of service used, the amount of data transferred, the traffic information of the calls made over their infrastructure. A prominent case of mass surveillance concerns the Centralized Monitoring System that is managed via Information and Communication Technologies Authority (ICTA), known as “*Bilgi Teknolojileri ve İletişim Kurumu*” (BTK), and enables the monitoring of all phone and internet communications. In 2020, it was alleged by a Member of the Grand National Assembly of Türkiye that the BTK requested internet service providers to send internet traffic records of all users (e.g., name, surname of the subscriber, IP numbers, location data) to it hourly by providing a detailed technical document about the requested type and format of the data²³³. HRW notes that widely used social media platforms [REDACTED] have complied with a 2020 legal amendment requiring them to establish offices in Türkiye, raising concerns that they will be forced to increase their compliance with government censorship in the future in order to avoid heavy fines and other penalties²³⁴.

2.2.1.3 PERSONAL DATA PROTECTION IN TÜRKİYE

Apart from the overarching protection provided to privacy and personal data of individuals in the Turkish Constitution, there are other laws which provide specific, sometimes context-dependent, protection measures. For example, the Turkish Criminal Law numbered 5204 (TCL) punishes certain misuses of personal data and brings dissuasive penalties under Article 134 (violation of privacy and secrecy), Article 135 (illegal recording of data, violation of data collection law, data collection without consent), 136 (illegal transfer and dissemination of personal data) and 138 (non-destruction of data). The Turkish Personal Data Protection Law (TPDPL)²³⁵ applies since 7 April 2016. Consequently, certain personal data processing operations are subject to the obligations and safeguards arising from the TPDPL. Article 4 TPDPL obliges data controllers and processors to comply with specific data protection principles such as lawfulness, accuracy, purpose and storage limitation, which align with the data protection principles enshrined in Article 5 GDPR. Furthermore, Article 11 TPDPL entitles data subjects to specific data subject rights including but not limited to the ones referred to in the Article 20 of the Constitution, namely the right to object to automated decision-making and the right to information about any international transfers of the data.

The TPDPL establishes the Personal Data Protection Supervisory Authority (SA) as a public independent institution by ensuring its financial and administrative autonomy in Article 19 and defines a set of general duties under Article 20.²³⁶ Moreover, the Personal Data Protection Board (the Board),

²³² The similar obligation is imposed upon internet access providers and hosting service providers. For the access service provider, the duration of traffic data is one year in Article 15(1)(b) of Regulation on Procedures and Principles Relating to Authorization to Access Providers and Hosting Providers. For hosting service provider the mandatory retention is six months (Article 16(1)(c) of the same Regulation), available at:

<https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=7&MevzuatNo=11679&MevzuatTertip=5>.

²³³ See, Medyoscope, *BTK-gate: Internet activity, identity, and personal data of all users in Turkey has been collected by BTK for the past year and a half*, available at: <https://medyoscope.tv/2022/07/21/btk-gate-internet-activity-identity-and-personal-data-of-all-users-in-Türkiye -has-been-collected-by-btk-for-the-past-year-and-a-half/>.

²³⁴ Human Rights Watch, *Turkey: YouTube Precedent Threatens Free Expression*, available at:
<https://www.hrw.org/news/2020/12/19/turkey-youtube-precedent-threatens-free-expression>.

²³⁵ The Turkish Personal Data Protection Law (TPDPL), numbered 6698, English version, available at:
<https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law>.

²³⁶ See, the Activity report for 2017-2022 published by the Turkish SA, “*5. yılında Kişisel Verileri Koruma Kurumu*”, 23 November 2022, available at: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/b5731c6c-540b-45eb-a2d8-d7cef57cf197.pdf>.

which is the decision-making body of the SA, was established pursuant to Article 21²³⁷. Among other duties and powers, the Board can issue administrative fines based on the criteria set in Article 18 in cases where the TPDPL is violated. However, the framework that establishes the Turkish SA and the Board has been criticised in EU progress reports due to a lack of safeguards for their respective independence²³⁸. In order to comply with the EU acquis, amendments to the TPDPL were proposed by the Turkish SA and legislative procedures are still ongoing at the time of drafting this report.

With respect to international personal data transfer, Article 9 TPDPL sets criteria for the transfer of personal data to countries outside of Türkiye and brings additional obligations for data controllers and processors. The TPDPL allows international personal data transfer in three instances (i) obtaining the explicit consent of the data subject; (ii) the country to which personal data will be sent has an adequate level of protection²³⁹; or (iii) in case, adequate protection is not provided, the data controllers in Türkiye and in the target country undertake such protection with an agreement in writing and obtain the approval of the Board²⁴⁰. At the time of writing this report, no country with adequate protection has so far been designated by the Turkish SA. Since the adoption of the TPDPL, the Turkish SA has published a number of information notes to provide further guidance on several aspects related to the application of TPDPL, including the international personal data transfer together with legal documents related to the model contractual clauses and binding corporate rules (BCR)²⁴¹. In 2018, the Turkish SA published two model clauses, similar to the standard contractual clauses (SCCs) under the GDPR, one for data transfers from a data controller to data controller, and one from a data controller to a data processor²⁴². However, unlike the GDPR, the TPDPL obliges data controllers to seek approval from the Board after they conclude the model clauses in order to have a valid legal basis for international data transfer²⁴³. Moreover, as announced by the Scientific Committee working on amendments of the TPDPL, the international personal data transfer rules will be updated in line with the GDPR rules²⁴⁴. For the moment, there is little official information available online about the scope and present status of the proposed TPDPL modifications.

Although the TPDPL provides specific safeguards for personal data processing in Türkiye, according to exceptions in the law, personal data could be processed and stored if it was a matter of national security. As such, Article 28 TPDPL excludes the law enforcement and national security domain from its scope together with the “*personal data (that) are processed by judicial authorities or execution authorities regarding investigation, prosecution, judicial or execution proceedings*”. An action for the annulment of some Articles including the provision of Article 28 TPDPL was filed with the Constitutional Court. The Constitutional Court rejected the action and found that the processing of personal data within the scope of preventive, protective and intelligence activities regulated in subparagraph (ç) of Article 28

²³⁷ According to the Article 22 TPDPL, the Board consists of nine members, of which five shall be elected by the Grand National Assembly of Türkiye; four members shall be elected by the President of the Republic of Türkiye with certain election procedures.

²³⁸ The EU Progress Report 2022 states that the lack of compliance of personal data protection rules with the acquis is an obstacle to data sharing and co-operation in many areas, in particular, in the context of Europol and Eurojust, p. 32.

²³⁹ Pursuant to Article 9(3) TPDPL, the Board shall declare the countries having adequate level of protection.

²⁴⁰ Article 9 TPDPL.

²⁴¹ See with regard to notes published by the Authority on *International Data Transfer*, available at:

<https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim>, <https://www.kvkk.gov.tr/Icerik/4106/Kisisel-Verilerin-Yurtdisina-Aktarilmasi>, <https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim>, and <https://kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU>.

²⁴² See, The Turkish SA, *Yurtdisina Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhutnamede Yer Alacak Asgari Unsurlar*, 2018, available at: <https://kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktarımında-VeriSorumlularınca-Hazırlanacak-Taahhutnamede-Yer-Alacak-AsgariUnsurlar>.

²⁴³ See, The Turkish SA, *Bağlayıcı Şirket Kuralları Hakkında Kamuoyu Duyurusu*, 10 April 2020, available at: <https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU>.

²⁴⁴ See, Presidency of Türkiye, *Human Rights Action Plan (2021-2023)*, Circular 2021/9, available at: https://insanhaklarileyemlani.adalet.gov.tr/resimler/%C4%B0nsan_Haklar%C4%B1_Eylem_Plan%C4%B1_ve_Uygulama_Takvimi.pdf.

TPDPL is in accordance with the Constitution while certain safeguards against those activities are envisaged in other specific laws²⁴⁵.

It can be argued that although there are certain safeguards provided in different laws, the safeguards against the interference with privacy and data protection rights are rather fragmented²⁴⁶, as will be further explored in the following section²⁴⁷. It is important to note that Turkish law does not regulate law enforcement use of data in a similar manner to how it is regulated in the EU by the Law Enforcement Directive. There is thus no separate legal instrument on personal data processing by law enforcement authorities²⁴⁸. However, in addition of the guarantees for privacy and data protection rights provided by the Constitution, certain safeguards can still be found in secondary legislation setting out the powers and duties of competent authorities (i.e. MIT Law, Police Law, Gendarmerie Law and Criminal Procedure Law), particularly, in the context of law enforcement and national security, as also further examined in detail in the next section

2.2.2 GOVERNMENTAL ACCESS TO PERSONAL DATA

2.2.2.1 GOVERNMENTAL ACCESS FOR NATIONAL SECURITY PURPOSES

There are three main intelligence organisations in Türkiye. First, the *Millî İstihbarat Teşkilatı* (MIT) (National Intelligence Organization) is responsible for providing intelligence related to national security, counter-intelligence activities and combating terrorism activities. Second, the General Directorate of Security²⁴⁹, which forms part of the Ministry of Interior, is mandated to carry out intelligence activities to protect national security as well as to ensure general security and public order at the national level²⁵⁰. For this purpose, it collects and evaluates information and conveys the intelligence data to relevant public authorities²⁵¹. Third, the Gendarmerie of General Command²⁵² is responsible for the intelligence activities to combat terrorism. Regarding the territorial competence of these organisations, while the MIT and the General Directorate are competent at the country level, the Gendarmerie has competence in the rural areas where there is no police force (the General Directorate). In other words, the Gendarmerie is responsible for the areas outside the municipal boundaries of provinces and districts where there is no police force²⁵³. In the following paragraphs, the report describes the competences and tasks of each these organisations in light of their relevance for personal data processing, underlining also any applicable safeguards, including oversight and redress mechanisms.

²⁴⁵ Atlı, T., *Kişisel Verilerin Önleyici, Koruyucu Ve İstihbari Faaliyetler Amacıyla İşlenmesi*, 2 Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, 2019, pp. 16-17, available at:

<https://dergipark.org.tr/tr/pub/neuhfd/issue/46494/579600>. See also the decision of the Constitutional Court. AYM, E.2016/125., K.2017/143., Karar Tarihi: 28.09.2017 E.T: 03.05.2019, paragraphs 151-159, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/143?KararNo=2017%2F143>.

²⁴⁶ The fragmented safeguards mean the safeguards mentioned in the study. See the list of legal instruments concerning the right to privacy and data protection. Kaya, M.B. F. Tastan, *Kişisel Veri Koruma Hukuku: Mevzuat & İctihat & Bibliyografya*, online, version 2.5, pp. 1774-1776, available at: <https://mbkaya.com/kisisel-veri-koruma-hukuku-mevzuat-ictihat/>.

²⁴⁷ See in particular sub-sections 2.2.2.4 and 2.2.2.5.

²⁴⁸ Moreover, there is also substantial ambiguity on the limits of personal data processing by law enforcement, gendarmerie or intelligence services, in particular with regard to the inadequacy of legal barriers and safeguards against a broad interpretation of national security by security agencies. Therefore, it is argued that the legal safeguards provided against security agencies are lacking clear-cut limits for the processing of personal data by such authorities. See, Ünver, H.A., Kim G., ‘Data Privacy and Surveillance in Türkiye’, *EDAM Cyber Policy Paper Series 2*, 2017, p. 29.

²⁴⁹ Law on the Duties and Powers of Police dated 1934 and numbered 2559 (Police Law), available at: <https://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf>.

²⁵⁰ Add. Article 7 (1) of Police Law.

²⁵¹ Add. Article 7 of Police Law.

²⁵² Law on the Duties and Powers of the Gendarmerie Organization dated 1983 and numbered 2803 (Gendarmerie Law), available at: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2803.pdf>.

²⁵³ Article 10(1) of Gendarmerie Law.

Personal data access by the National Intelligence Organisation (MIT)

Tasks and competences of the MIT

The MIT is responsible for providing intelligence related to national security, counter-intelligence activities and combating terrorism activities. The tasks and competences of MIT are stipulated in the Law numbered 2937 on the State Intelligence Services and the National Intelligence Organization (MIT Law)²⁵⁴. Article 4 of the MIT Law explicitly determines the scope of the tasks of the MIT. Article 4(1) stipulates ten different tasks of the MIT. These tasks can be divided into five categories providing intelligence regarding: (i) the protection of national security and state security, (ii) combating terrorism²⁵⁵, (iii) combating international crimes²⁵⁶ and cybercrimes²⁵⁷, (iv) coordinating intelligence activities with other public authorities, and (v) improving the organisational and technical capacity for the aforementioned tasks. For carrying out the tasks given to MIT, MIT is equipped with the necessary competences and powers. Article 6 of MIT Law sets forth the competences of the MIT. For the report, the following three competences and powers of MIT are relevant because it might lead to the access of personal data by the MIT: (i) the power to request information and documents from public institutions and organisations as well as private entities (Article 6(1)(b)); (ii) the power to access the databases on entry and exit of foreigners, granted visas, residence permits, work permits and deportations (Article 6(1)(f)); and (iii) access to data in communication (Article 6(1)(h)).

Regarding the power to request access to information and documents held by public entities, Article 5(1) of the MIT stipulates that all public entities are responsible for providing intelligence and information to the MIT within the scope of their respective tasks. Furthermore, Article 6(1)(b) of the MIT Law states that all public entities shall respond to MIT's requests. However, if public entities consider a request unlawful due to its excessive nature, they might refuse it on the basis of its illegality. Regarding the request for access to information and documents held by private entities, the MIT can address its request to all private entities that are established in Türkiye. The scope of the private entities that can be the subject of such requests are delineated in Article 6(1)(b). According to this paragraph, the MIT can request information, documents, data and records from institutions and organisations within the scope of the Banking Law dated 19/10/2005 and numbered 5411, as well as other legal persons and institutions without legal personality, and use their telecommunication infrastructure or data processing centres. The MIT can request access to their archives, electronic data processing centres and communication infrastructure, and may contact them. In this context, private or public entities cannot avoid the fulfilment of the request by referring to other laws that apply to these private entities. Yet, as will be discussed in section 2.2.2.3, almost all administrative actions are subject to judicial review according to Article 125 of the Constitution. Thus, the legality of the request can be challenged before the administrative courts.

Substantial and procedural conditions and safeguards for personal data access

The powers of access of the MIT can include personal data if the access is related to the activities of human intelligence and signal intelligence in particular, which can be related to a natural person. The procedural and substantial conditions that protect personal data vary depending on the type of power used.

²⁵⁴ Law 2937 on The State Intelligence Services and the National Intelligence Organisation, available at: <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2937&MevzuatTur=1&MevzuatTertip=5>.

²⁵⁵ With regard to counter-terrorism capacity and framework of Türkiye, see Council of Europe Committee on Counter-terrorism (CDCT), *Profiles on Counter-Terrorism Capacity: Türkiye*, available at: <https://rm.coe.int/profile-november-2022-Turkey/1680a94979>.

²⁵⁶ While there is no definition of international crimes in MIT Law, the crime of genocide (Article 76), the crime against humanity (Article 77), the crime migrant smuggling (Article 79) and of human trafficking (Article 80) are incorporated in the TCL numbered 5237 (in Turkish), available at:

<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5>. See for the analysis of international crimes in TPC in the light of Rome Statue: Erhan, Z. (2019), *Core International Crimes In Turkish Criminal Law And The Rome Statute*, 22 Haci Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Ankara, p. 111.

²⁵⁷ Cybercrimes can be found in Articles 243- 245 of the TCL.

For information requests to public and private entities under Article 6(1)(b), the scope of information access is restricted to the tasks of the MIT as defined in Article 4 of the MIT Law. There are no further conditions described in the MIT Law for such access, but the safeguards mentioned in the following paragraph also apply. Additional substantial and procedural conditions of information accessed by the MIT are supposed to be further specified by a regulation issued by the Presidency of Türkiye following Article 6(10) of the MIT Law. However, the regulation that specifies these conditions is not published in the official journal and is not accessible to the public in line with Article 32 of MIT Law. Nevertheless, it should be borne in mind that a restriction of fundamental rights is only possible by a law that is adopted by the Grand National Assembly of Türkiye according to Article 13 of the Constitution²⁵⁸. Thus, while the regulation might substantiate or clarify the conditions and safeguards mentioned in the MIT Law, these clarifications in the regulation adopted by the Presidency of Türkiye cannot restrict the right to data protection or other fundamental rights due to Article 13 of the Constitution.

The MIT Law provides general safeguards for situations when the MIT accesses and uses information. These safeguards apply to all measures taken by the MIT unless specifically exempted. The first safeguard is the confidentiality requirement imposed upon the MIT in Article 6(6) of the MIT Law²⁵⁹. The second safeguard is purpose limitation. Article 6(6) states that neither the record nor the information can be used for any purposes other than the tasks mentioned in Article 4 of the MIT Law²⁶⁰. Furthermore, the information possessed by the MIT cannot be requested by the Court except for crimes related to state secrets and espionage²⁶¹ according to Additional Article 1 of the MIT Law²⁶². The third safeguard is that the unauthorised obtaining, stealing, faking or destruction of information or documents possessed by the MIT is criminalised in Article 27 of the MIT Law²⁶³. A person that commits one of the acts listed can be sentenced to imprisonment for four to ten years. If a person that is affiliated with the MIT commits such a crime, the imprisonment to be imposed is increased by up to one-third.

The access to information by the MIT has been criticised by the HRW due to the lack of protection of privacy and data protection²⁶⁴. The constitutionality of Article 6(1)(b) of the MIT Law has been assessed by the Constitutional Court of Türkiye²⁶⁵ on the allegation of its incompatibility with the Constitution including Article 20 of the Constitution (right to privacy and data protection). The Court acknowledged that the powers granted to the MIT in Article 6(1)(b) constitute an interference with Article 20, which guarantees the right to privacy and right to data protection. The majority of the members of the Court found this interference (request of information access by the MIT) necessary and proportionate because there are appropriate safeguards, noting the safeguards mentioned in the previous paragraph and the internal oversight within the MIT, the ex-post oversight mechanism of the “State Supervisory

²⁵⁸ Article 13 of the Turkish Constitution requires restrictions to fundamental rights to be “provided by law”. This “provided by law” element is only met by a legislation adopted by the General Assembly. For instance, a presidential decree mandates the request of information and document by the MASAK (the authority responsible for combating anti-money laundering and terrorist financing). The Constitutional Court stated that it is only possible to restrict fundamental rights (right to data protection) by a legislation but not with a presidential decree. See AYM, E.2019/96, K.2022/17, 24/02/2022, paragraph 63 and following paragraphs, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/17>.

²⁵⁹ AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 26, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁶⁰ Ibid.

²⁶¹ See Articles 326-339 of the TCL.

²⁶² AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 27, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁶³ AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 27, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁶⁴ Human Rights Watch, *Türkiye Spy Agency Law Opens Door to Abuse*, available at: [https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse#:~:text=\(Istanbul\)%20%E2%80%93%20A%20new%20law,an%20the%20right%20to%20privacy](https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse#:~:text=(Istanbul)%20%E2%80%93%20A%20new%20law,an%20the%20right%20to%20privacy).

²⁶⁵ AYM, E.2014/122, K.2015/123 T. 30/12/2015, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>

Council”²⁶⁶ and the parliamentary oversight²⁶⁷, as well as the legal redress mechanisms which will be discussed further below²⁶⁸. A dissenting opinion did not agree²⁶⁹ and stated that the broad scope of power to request the information might force private entities to show incriminating evidence against themselves or their relatives or to provide information, documents, data, and records learned as a result of their profession and containing secrets such as in the context of a lawyer-client relationship²⁷⁰. In addition, the dissenting opinion underlined that the rule of law required public authorities to protect fundamental rights and freedoms when interfering with them for security purposes²⁷¹. If the MIT is granted a broad authorisation for national security purposes, it should be foreseen that it can be used in cases directly related to the task, limited to the request, and necessary measures should be taken to protect these limits and prevent misuse²⁷².

Additional substantial and procedural conditions are set to limit the power in terms of access to communication data (metadata), content, and signal detection, in addition to the safeguards mentioned. The safeguards available in situations where there has been national security government access vary depending on whether the individuals that are subject of the measure are foreign or whether they are residing in Türkiye or abroad.

The following eight safeguards apply to Turkish citizens that reside in Türkiye.

- The first safeguard of a substantial nature is laid down in Article 6(2) of the MIT Law and states that access to personal data must be justified by a serious threat to national security, revealing espionage activities, preventing the disclosure of state secrets, or combating terrorism.
- The second safeguard of a procedural nature is that an order of a judge of the Assize Court in Ankara in Türkiye is required (Article 6(3) of the MIT Law). In case of urgent need, the President of the MIT or the Vice-President can order access, but the approval of a judge is required within 24 hours. If the judge does not approve the order or does not make the approval within 24 hours, then the order is deemed to be revoked.
- The third safeguard is a requirement for the order to include specific elements listed in Article 6(4). In the written order or judicial decision, the identity of the person to whom the measure will be applied, the type of communication tool, the telephone numbers, the type of measure, the scope and duration of the measure and the reasons for applying the measure have to be specified.
- The fourth safeguard in the same paragraph is the duration of the measure. The order or decision for the specific measure has to be limited to three months at one time. The measure can be extended a maximum of three times. This maximum time limit does not apply to access to content and metadata of the communication for the purpose of detecting espionage activities or combating terrorism.
- The fifth safeguard is that the measure is implemented in a specific place within the BTK or established by MIT according to Article 6(2) of MIT Law.
- The sixth safeguard is related to the destruction of the content of the communication. If the access measure is terminated, the recordings of the accessed content have to be destroyed within ten days at the latest. Affected organisations must be able to demonstrate compliance with this rule by making a report on the matter and safekeeping it so that it can be submitted in case of an audit.

²⁶⁶ AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 31, available at:

<https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁶⁷ AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 32, available at:

<https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁶⁸ See Section 2.2.2.

²⁶⁹ See Dissenting Opinion of Alparslan Altan and Erdal Tezcan, in particular paragraphs 1-19, AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 32, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁷⁰ See paragraphs 13-14 of the Dissenting Opinion of Alparslan Altan and Erdal Tezcan, AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 32, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁷¹ Ibid, paragraph 18.

²⁷² Ibid.

- The seventh safeguard is to record the log details of the measures in a report. The report contains the start and end time of the measures as well as the identity of the person performing the measure according to Article 6(7).
- The eighth safeguard is that if the MIT does not meet the aforementioned legal requirements while applying the measure, the evidence obtained via these measures can be considered unlawful and the persons that do not comply with these conditions can be prosecuted in accordance with the TCL according to Article 6(9) of the MIT Law.

In terms of communication data (metadata), content of communication, and signal detection for communications abroad regardless of the nationality of the affected persons or of foreigners in Türkiye, the general safeguards mentioned apply to this measure (purpose limitation, confidentiality requirement etc.)²⁷³. However, the specific safeguards within the MIT Law are limited in comparison with the safeguards described in the previous paragraph. To carry out its tasks in Article 4, the MIT can listen to communications or detect and evaluate signal information to obtain preventive intelligence and make an analysis with the approval of the President or Vice-President of the MIT. The necessity and proportionality requirements for this measure are not specifically mentioned in Article 6(11), though even then the necessity and proportionality requirements for fundamental rights laid down in Article 13 of the Constitution need to be respected. This was discussed in the case of *Bestami Eroğlu* by the Constitutional Court, which is further explained below²⁷⁴. The information and data processed within these activities can only be used for intelligence activities and cannot be used for other purposes including as a basis for criminal prosecutions²⁷⁵.

The constitutionality of Article 6(11) of the MIT Law was assessed by the Constitutional Court of Türkiye, on the basis of an alleged violation of, among others, Article 20 (right to private life and data protection) as well as Article 22 of the Constitution (right to the confidentiality of communication)²⁷⁶. The Court found it compatible with fundamental rights by referring to the general safeguards mentioned in Article 6(1)(b)²⁷⁷. In the dissenting opinion, [REDACTED] some judges disagree with the majority stating that the absence of specific safeguards mentioned for Turkish citizens living in Türkiye cannot be justified and violates the right to the confidentiality of communication and refers to *Klass and other v. Germany* case of European Convention of Human Rights (ECtHR)²⁷⁸. In addition, they underline the importance of ex-ante judicial review for interference with the confidentiality of communication²⁷⁹.

The Constitutional Court has assessed the legality of the personal data access by the MIT in the complaint of *Bestami Eroğlu*. This complaint was related to the access to personal data by MIT and further use by the Courts in the criminal investigation and prosecution in this specific complaint²⁸⁰. The Court explicitly stated that while the derogations from the right to data protection is possible for the purpose of national security and crime prevention, the interference with right to data protection by public authorities shall meet the legality, necessity and proportionality requirements foreseen under Article 13 of the Constitution²⁸¹. Referring to the powers of the MIT in the paragraphs mentioned above, the Court reiterated that the MIT Law meets the legality requirement. In the specific analysis of facts, the Court

²⁷³AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 32, available at:

<https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

See the complaint of Bestami Eroğlu for the legal analysis of further process by judicial authorities in the criminal prosecution, *Bestami Eroğlu* [GK], B. no: 2018/23077, T. 17/9/2020, available at:

<https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/23077?BasvuruAdi=BESTAM%C4%B0+ERO%C4%9ELU>.

²⁷⁴Ibid., paragraph 139.

²⁷⁵AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 80, available at:

<https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁷⁶Ibid., paragraph 32.

²⁷⁷Ibid., paragraph 80.

²⁷⁸ See the dissenting opinion of [REDACTED], AYM, E.2014/122, K.2015/123 T. 30/12/2015, available at:

<https://nomkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

²⁷⁹Ibid.

²⁸⁰*Bestami Eroğlu* [GK], B. No: 2018/23077, T. 17/9/2020, available at:

<https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/23077?BasvuruAdi=BESTAM%C4%B0+ERO%C4%9ELU>.

²⁸¹Ibid., paragraph 145.

analysed whether the access to personal data in the *Bylock* application²⁸² by the MIT and to data processed (communication data) by BTK is necessary and last recourse to pursue the aim of detecting members of terrorist organisations, which prejudices national security. The Court stated that the access to data (IP addresses, the content of message and telephone records) by deploying intelligence techniques by MIT cannot be considered as incompatible with the necessity requirement²⁸³. With respect to the proportionality element, the Court required four safeguards in the government data access: (1) limited use of data for the purpose of national security, (2) not excessive retention of data (3) not merely using this data for the legal consequences (criminal conviction) and (4) effective judicial redress mechanism²⁸⁴. The Court decided that these safeguards are respected in the specific case and find the interference with the right to data protection and right to confidentiality of the communication compatible with the Constitution²⁸⁵.

Personal data access by the General Directorate of Security and Gendarmerie of General Command

Tasks and competences of the General Directorate of Security and Gendarmerie of General Command

There are two powers of the Directorate and Gendarmerie related to personal data processing: access to information and documents held by public entities²⁸⁶ and access to metadata and content of communication as well as signal detection²⁸⁷.

Substantial and procedural conditions and safeguards for personal data access

Regarding information access, in contrast to the MIT's power, the Directorate and Gendarmerie can only request information and documents from public entities. Thus, the Directorate and Gendarmerie cannot request information from private entities. The general safeguards are similar to the general safeguards mentioned for the MIT's access to information and documents. In contrast to the powers of the MIT, the request has to be in writing and the Directorate has to justify its request. In addition, the Directorate shall get judicial approval if the public entities refuse to provide information based on incompatibility with the law in general, as well as trade secret reasons. Concerning access to telecommunication data as well as the content of communication, the safeguards converge with the safeguards for the MIT's power of access to telecommunication data. In contrast to the MIT's competences, there is no difference between foreigners and citizens in terms of safeguards. They have the same safeguards. The only difference with the conditions mentioned in the section for the MIT is that in case of urgency, judicial approval shall be taken within 48 hours rather than 24 hours.

2.2.2.2 OVERSIGHT MECHANISM FOR NATIONAL SECURITY ACCESS

The data processing activities by the intelligence organisations are not subject to the oversight of the Turkish SA due to Article 28 TPDPL. However, there are three *ex-post* external oversight mechanisms, which are relevant for intelligence activities. These oversight mechanisms apply to all intelligence activities unless it is stated otherwise.

The first is the administrative oversight by the State Supervisory Council, known as “*Devlet Denetleme Kurulu*” (DDK)²⁸⁸. The Council is a constitutional institution established within the Presidency, which

²⁸² [REDACTED]

²⁸³ Bestami Eroğlu [GK], B. no: 2018/23077, T. 17/9/2020, paragraph 148, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/23077?BasvuruAdi=BESTAM%C4%B0+ERO%C4%9ELU>.

²⁸⁴Ibid, paragraph 153.

²⁸⁵Ibid, paragraph 158.

²⁸⁶ Add. Article 7(6) of Police Law and Add. Article 5(5) of Gendarmerie Law.

²⁸⁷ Add. Article 7(2) of Police Law and Add. Article 5(1) of Gendarmerie Law.

²⁸⁸ Article 6(8) of MIT Law; add. Article 7(9) of Police Law and Article 5(8) of Gendarmerie Law.

is responsible for the oversight of public entities except for judicial bodies and has the power of investigation, examinations and inspections according to Article 108 of the Constitution. The president and members of the Council are appointed by the President²⁸⁹. Its powers are further specified in the Presidential Decree on the State Supervisory Council²⁹⁰. While the Council itself does not have corrective powers, based on its investigations and inspections, the Council can prepare reports and inform the prosecutors or relevant public entities to initiate judicial procedures if any irregularities are found²⁹¹. This oversight mechanism is not open to public scrutiny.

The second *ex-post* external oversight mechanism is parliamentary oversight. The Security and Intelligence Committee has been established within the Grand National Assembly of Türkiye²⁹². Annual reports have to be prepared by the MIT, the Directorate and the Gendarmerie, and are sent to the Presidency²⁹³. The annual report shall be submitted to the Security and Intelligence Committee each year. The Committee consists of 17 members according to the representation of political parties in the National Assembly²⁹⁴. The report that is provided to the Committee and the deliberations within the Committee are confidential²⁹⁵. One of the tasks of the Committee is to provide recommendations to protect the security of personal data obtained during security and intelligence services and the rights and freedoms of individuals. The EU progress report on Türkiye states that the oversight of security and intelligence organisations by the parliament must be strengthened considering the limited accountability of the police and security organisations²⁹⁶. The activities of the Committee are considered as confidential and not open to public scrutiny.

The third oversight mechanism is oversight by the Ombudsman, which was established in 2012 as a constitutional public entity affiliated with the Grand National Assembly of Türkiye²⁹⁷. It is an independent and impartial institution, which is tasked with investigating administrative practices and making recommendations to the administration in terms of compliance with the law in particular human rights' standards²⁹⁸ based upon a complaint mechanism. Everyone has a right to file a complaint against the administrative act or decision according to Article 74(4) of the Constitution. The right to a complaint is granted to everyone, therefore, foreigners can also initiate a complaint against administrative acts or decisions if foreigners are affected by said decision or act.

The oversight by the Ombudsman is not specifically designed for government access to personal data for intelligence purposes. However, its scope is broad enough to extend to such data access according to Article 5 of the Law on the Ombudsman Institution numbered 6328 and dated 2012. As the right to data protection as well as the right to privacy are human rights recognised in the Turkish Constitution, the Ombudsman has the power of access to information and documents and of proposing non-binding recommendations to public entities, if they infringe the right to data protection or other fundamental rights. If the concerned public entity does not comply with the recommendation, it has to justify its non-compliance. For example, the Ombudsman issued a recommendation on the processing and storing of

²⁸⁹ See for a criticism against the independence of the Council with respect to anti-corruption matters, EU Progress Report, 2022, p. 28.

²⁹⁰ Presidential Decree on Devlet Denetleme Kurulu numbered 5 dated 15/07/2018, available at: <https://www.mevzuat.gov.tr/MevzuatMetin/19.5.5.pdf>.

²⁹¹ Ibid, Article 20.

²⁹² Additional Article 2(1) of the MIT Law. See for the critical analysis of the oversight regime: Olgunsoy, F. (2019), *The Impact Of Intelligence Activities In Fight Against Terror On Liberties: Turkey, United Kingdom, United States Of America* (PhD Thesis in Turkish), available at: <http://nek.istanbul.edu.tr:4444/ekos/TEZ/60634.pdf>.

²⁹³ Add. Article 2(1) of MIT Law; Add. Article 7(9) of Police Law and Article 5(8) of Gendarmerie Law.

²⁹⁴ Add. Article 2(3) of MIT Law.

²⁹⁵ Add. Article 2(6) of MIT Law, see the suggestion of the publication of the report, Olgunsoy, F. (2019), *The Impact Of Intelligence Activities In Fight Against Terror On Liberties: Turkey, United Kingdom, United States Of America*(PhD Thesis in Turkish), available at: <http://nek.istanbul.edu.tr:4444/ekos/TEZ/60634.pdf>.

²⁹⁶ EU Commission, *Türkiye 2022 Report*, pp. 5 and 17, available at: <https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf>.

²⁹⁷ Article 74 of the Constitution.

²⁹⁸ See the analysis of the Institution and its impact on fundamental rights, Alyanak, S., *The New Institution on Protection of Fundamental Rights: Turkish Ombudsman Institution*, available at: <https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/42699>.

personal data of sensitive nature (criminal records) in the law enforcement database by the General Directorate of Security²⁹⁹.

The Ombudsman received certain criticisms in the EU Progress Reports. The first one is that it does not have ex-officio investigation power and cannot issue legally binding decisions against public entities³⁰⁰. The second criticism is its silence on critical fundamental rights concerns³⁰¹. Therefore, its oversight over the governmental data access might be considered limited.

2.2.2.3 JUDICIAL REDRESS MECHANISMS FOR NATIONAL SECURITY ACCESS: ADMINISTRATIVE, CRIMINAL AND CONSTITUTIONAL LAW REMEDIES

Individuals can exercise judicial redress mechanisms in administrative and constitutional law. As a requirement of the rule of law, an administrative action, which refers to any decision or action taken by an administrative authority in the exercise of its official powers, shall be subject to judicial review. Article 125 of the Constitution stipulates that judicial remedy is open against all kinds of acts of public entities. The acts of public entities are subject to the jurisdiction of the administrative and tax courts. Judicial review of the legality of the acts of the administration is ensured through annulment action and full compensation action.

An annulment action is a judicial process that checks whether the administrative action is unlawful. According to Article 2(1)(a) of Administrative Procedure Law of Türkiye³⁰², everyone including foreigners can initiate the annulment action if they meet the following conditions: (i) violation of interest, (ii) the existence of final and executable action, and (iii) exercise of the action within sixty days. For government data access, the annulment action can be used as long as these three conditions are met. The violation of data protection rights can be considered a violation of interest since data protection is considered a fundamental right under Article 20 of the Constitution. Data access by intelligence organisations is less likely to meet the second condition unless the processing of personal data leads the public entities to initiate a final and executable action against a natural person³⁰³. For instance, if the residence permit application of a foreign individual is denied based on personal data processing for intelligence purposes, the foreign individual can seek the annulment of a decision on the residence permit application. In this example, the reasoned decision of the administrative authority might refer to national security as a reason for the denial of the residence permit. If the foreign individual can seek the annulment of the decision on the residence permit application, during the proceedings, the Administrative Court can request the relevant information and review the legality of the decision and take into account the right to data protection as it is recognised as a fundamental right under Article 20 of the Constitution.

Individuals may also seek monetary compensation if administrative actions caused harm to individuals according to the Constitution³⁰⁴. For instance, in the individual complaint of *Yasemin Congar and others*,

²⁹⁹ Application no. 2019 4234, 23 August 2019, available at:

<https://kararlar.ombudsman.gov.tr/Arama/Download?url=20190219\19438\Yayin\Karar-2019-4234.pdf&tarih=2019-08-23T14:09:55.848612>.

³⁰⁰ EU Commission, *Türkiye 2022 Report*, p. 14.

³⁰¹ Ibid.

³⁰² The Administrative Procedure Law of Türkiye, numbered 2577, available at:

<https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2577.pdf>.

³⁰³ See for different decisions of the Administrative Court regarding the annulment actions in the case of personal data processing, Akman, N. G. (2021), *Protection of Personal Data by Administrative Law (Master Thesis)*, available at: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=v7BkNnepTnbhn8rNR77LcR_II-f_TK_3XoNmW2wSHu86pEYn4zgNqFITXoQxtnR.

³⁰⁴ Article 125 of the Constitution.

the Constitutional Court reward non-pecuniary damages to the complainants³⁰⁵. These non-pecuniary damages were awarded due to the violation of the right to the confidentiality of communications of the complainants. The violation occurred because while the MIT requested the judge to listen to the complainants' communications, the MIT did not write their real identities in the written request but wrote down a false identity to ensure the confidentiality of the investigations, which is against Article 6(4) of the MIT Law, which prescribes the indication of real names. The administration's non-contractual liability manifests itself in the form of faulty or strict liability. The procedure and conditions of seeking damages in administrative courts are regulated in the Administrative Procedure Law of Türkiye³⁰⁶. Regarding government data access, if the data is used for purposes other than those specified in the law, disclosed to third parties, and not deleted after the statute of limitations specified in the law, and as a result, the persons are exposed to material or moral harm, the administrative courts can require the state to pay damages to the individuals³⁰⁷.

According to Article 148(3) of the Constitution, everyone who enjoys the rights and freedoms guaranteed by the Constitution may file a complaint with the Constitutional Court alleging that any of their freedoms protected by the ECHR have been violated by the state. Before applying, it is required that all possible legal remedies have been exhausted. As personal data protection and the right to privacy are considered fundamental rights, individuals can seek monetary or non-monetary damages in case of a violation of their right to data protection. In addition, the Court can order a retrial if it is necessary. In terms of government data access, the processing of personal data by intelligence organisations may not be considered an action of a state with public force unless it has further consequences for individuals. This is because the processing of personal data by intelligence organisations is generally a preparatory action before state authorities take further action. Therefore, it is very rare for an individual applicant to use this individual complaint remedy against such actions of the intelligence agencies as an individual might not realise that an intelligence activity is being carried out against him or her.

However, it is not impossible, considering the following examples. For instance, in the complaint of *Ercan Kanar*, he claimed that the MIT unlawfully collected his personal information in an intelligence report and that this report contained information on his personal, private, and professional status, which was included in the criminal investigation. The complainant argued that the disclosure was against, among others, Article 20 of the Constitution (right to privacy and data protection). The Court held that a serious interference to the applicant's private life had occurred by making his personal information available via inserting the intelligence report into the case file³⁰⁸. The Court stated that in a democratic society, it was unacceptable to insert intelligence information that had not been requested in any way and had not been subject to review. It could not be justified as necessary in a democratic society, nor could it be justified as proportionate³⁰⁹. More importantly, individuals can complain when a decision or an action is taken against them and has a legal effect such as a denial of entry to Türkiye or the freezing of their assets. For example, if individuals initiate a request to exercise their right of access, as will be discussed further in section 2.2.4, then if this request is rejected by intelligence organisations, individuals can initiate the judicial redress mechanism mentioned in this section. If they are not satisfied with the decisions of the courts, they can invoke their right to personal data protection before the Constitutional Court. Therefore, individuals can complain about the violation of the right to data protection after they have exhausted all remedies in criminal courts or administrative courts as a last recourse³¹⁰. After the

³⁰⁵ AYM, *Yasemin Çongar ve diğerleri [GK]*, B. No: 2013/7054, 6/1/2015, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/7054>.

³⁰⁶ See Articles 12-13 of the Administrative Procedure Law of Türkiye.

³⁰⁷ See examples of actions for damages against the state in general, Akman, N. G. (2021), *Protection of Personal Data by Administrative Law* (Master Thesis), available at: https://tez.yok.gov.tr/UlusaltTezMerkezi/TezGoster?key=v7BkNnneptnbhn8rNR77LcR_II-f_TK_3XoNmW2wShu8epEYn4zgNqFITXoQxtnR.

³⁰⁸ AYM, *Ercan Kanar*, B. No: 2013/533, 9/1/2014, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/533>.

³⁰⁹ Ibid, paragraph 61.

³¹⁰ See for the analysis of potential victim in case of intelligence activities, Olgunsoy, F. (2019), *The Impact of Intelligence Activities In Fight Against Terror On Liberties: Turkey, United Kingdom, United States Of America* (PhD Thesis), pp. 181-182, available at: <http://nek.istanbul.edu.tr:4444/ekos/TEZ/60634.pdf>.

individual complaint mechanism, as Türkiye is a party to ECHR, it is also possible to initiate a complaint against Türkiye before the ECtHR.

2.2.2.4 GOVERNMENTAL ACCESS TO PERSONAL DATA FOR THE PURPOSE OF CRIMINAL INVESTIGATION AND PROSECUTION

Under Turkish Criminal Procedure Law (TCPL)³¹¹, various tools are available for prosecutors and courts to gather evidence during a criminal investigation or prosecution. In general, these measures are carried out by law enforcement agencies under the supervision of prosecutors or courts. The judge of the criminal court of peace, which is the court at the location of the prosecutor who has made the request at the investigation stage, is authorised to decide on the measures, and the court hearing the case is authorised during the prosecution stage.

Among others, prosecutors, judges or courts may request any information in writing during the investigation and prosecution of offences, pursuant to Article 332 TCPL. Furthermore, Article 161(2) TCPL obliges other public officials to provide the requested information and documents without delay upon the request made by the public prosecutor. In contrast to Article 332, Article 161(2) does not specify any formal requirements for the information request by the public prosecutor. As an important note, failure of public officials to respond to an information request or to provide information or documents may constitute a crime of misconduct under Article 257 TCL.

Two measures available to the public prosecutor stipulated under the TCPL are of relevance for this study: (i) search of computers, computer programs and transcripts, copying and provisional seizure³¹²; and (ii) interception of correspondence through telecommunication³¹³. Given the amount of personal data that may be accessed or processed through individuals' computers or communications via telecommunications, the remainder of this sub-section focuses on the conditions and safeguards provided by law for the application of these investigatory measures.

Search of computers, computer programs and transcripts, copying and provisional seizure

Article 134 TCPL allows for searching the computers, computer programs and computer logs used by a suspect, and for making copies of computer records and decoding and transcribing these records for the purpose of obtaining evidence during an ongoing investigation or prosecution. The provision provides additional safeguards for the suspects and accused such as during the seizure of computers or computer logs, all data in the system shall be backed up³¹⁴ and if requested by the suspect or his or her attorney, a copy of this backup shall be made and given to the suspect or his or her attorney, and this shall be recorded in a report and signed³¹⁵. A copy of all or part of the data in the system may be taken without seizure of the computer or computer logs. The copied data shall be printed on paper and this matter shall be recorded in the minutes and signed by the relevant persons³¹⁶. Following the amendment made to the provision in Article 16 of the Law No. 7145 dated 25 July 2018, additional safeguards and time limitations are introduced. In this vein, decisions issued by the public prosecutor shall be submitted for the approval of the judge within 24 hours. The judge shall render his or her decision within 24 hours at the latest. If the time limit expires or if the judge decides otherwise, the copies and transcripts shall be destroyed immediately³¹⁷.

³¹¹ The Criminal Procedure Law of Türkiye, numbered 5271 and dated 2004, available at:
<https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5271.pdf>.

³¹² Article 134 TCPL.

³¹³ Article 135 TCPL.

³¹⁴ Article 134(3) TCPL.

³¹⁵ Article 134(4) TCPL.

³¹⁶ Article 134(5) TCPL.

³¹⁷ This amendment is introduced as a safeguard in line with the Article 20 of the Constitution.

Interception of correspondence through telecommunication

Pursuant to Article 135(1) TCPL, the telecommunication of a suspect or defendant may be intercepted, recorded and signal information may be evaluated³¹⁸ with the decision of the judge or, in case there is urgency by the public prosecutor, to obtain evidence in relation to an ongoing investigation or prosecution of certain crimes. The provision requires the existence of a strong suspicion that certain crimes listed in the law have been committed as a condition for the application of the measure. In line with ECtHR case law³¹⁹, this measure can only be applied if it is impossible or very difficult to establish material facts by other means in order to prevent arbitrary practices. The provision states that the measure can be applied for a maximum period of three months, and it is foreseen that this period can be extended at most once. With the amendment made to the Article 135(3) TCPL, the duration of the measure may be extended several times for a period not exceeding one month each time, but no upper limit is foreseen for organised crimes. This measure is applied in secret, and therefore, it is not possible for the person against whom the measure is applied to be aware of it.

Under the same provision, Article 135(6) TCPL regulates the detection of a suspect's or defendant's telecommunications, i.e. Historical Traffic Search (HTS), independently of the other measures provided for in Article 135(1) TCPL³²⁰. The application of Article 135(6) is subject to similar safeguards deriving from Article 20 Constitution, such as the requirement of a judge's decision or, in urgent cases, the decision of the public prosecutor, provided that it is submitted to the judge within 24 hours. However, Article 135(6) TCPL does not require the strong suspicion or limited applicability to certain offences as a precondition for the applicability of this measure, as provided for in Article 135(1) TCPL. Thus, the detection of the suspect's or defendant's telecommunications may find wider scope of the application in criminal investigations and prosecutions compared to the measures stipulated under Article 135(1) TCPL³²¹.

As an additional safeguard, Article 136 TCPL stipulates that the communication of the suspect or defendant with his or her defence counsel cannot be monitored and intercepted. According to Article 137(4) TCPL, when the data obtained via this measure are destroyed, the Public Prosecutor's Office must inform the relevant person in writing about the reason, scope, duration and result of the measure within 15 days at the latest from the end of the investigation phase. In cases where the data obtained used in the investigation and a lawsuit is filed against the relevant person, the relevant person is not notified separately about the measure because, the indictment is notified to the person concerned, and the person concerned has learnt that the measure has been applied. In case the measure is applied at the prosecution stage, it is not possible to apply the measure secretly.

The procedural and substantial conditions and safeguards

Given the intrusiveness of the aforementioned measures and their potential implications on the fundamental rights, the legislator regulated these two measures as a “last resort” to obtain the evidence. In other words, if it is possible to obtain evidence by other means, in principle, these measures cannot be applied except the detection of the communication as stipulated under Article 135(6) TCPL. In this regard, other conditions and limitations are introduced in the provisions such as “limited duration” of the measure, “transcribing records” and all the data obtained, and “if there are strong indications of suspicion that crime is attempted”. These measures might be applied in case there is “strong

³¹⁸ The TCPL does not specify whether historical traffic search (HTS) records that were retained by telephone operators “prior to the date of the decision” can be requested or used in the ongoing investigation or prosecution of a crime.

³¹⁹ Judgment of the European Court of Human Rights of 6 September 1978, *Klass and ors v Federal Republic of Germany*, Judgment, Merits, no 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978).

³²⁰ Article 135(6) TCPL.

³²¹ Article 135(5) TCPL also regulates a specific measure for the determination of the location of suspects of defendants' mobile phone in order to catch them, based on the decision of the judge or in case there is urgency with the decision of the prosecutors, without the need for seeking judges' approval. This measure also can be applied maximum of three months.

suspicion”³²² that one or more of the offences listed in the relevant provisions have been committed. It means that a simple suspicion is not sufficient for the application of these measures. In case, there is urgency, those measures can be initiated by the decision of the public prosecutor alone, with the condition that the rendered decision shall be submitted for the approval of the judge within 24 hours and the judge shall decide in 24 hours at the latest. Those measures expire in the event of a decision of non-prosecution or the termination of suspicion, the conclusion of the case, the disappearance of other conditions related to the measure, anytime with the decision of the prosecutor or in the event that the decisions made by the public prosecutor are not submitted for the approval of the judge within 24 hours or the cautionary decisions submitted for approval are not decided by the judge within 24 hours and are not approved by the judge. Based on the aforementioned conditions and safeguards, the Constitutional Court also found some of these measures proportionate, legitimate and compliant with the Constitution³²³.

2.2.2.5 JUDICIAL REDRESS MECHANISMS IN CASE OF LAW ENFORCEMENT ACCESS TO PERSONAL DATA

The application of the measures explained in section 2.2.2.4 without a judge’s decision or, in exceptional cases, a prosecutor’s decision is unlawful, and hence the data obtained in this way can neither be used as evidence nor form the basis of a judgment³²⁴. Moreover, the Court of Cassation also takes into account the absence of the judge’s decision regarding the surveillance of communication in the file, or not being submitted to the file, or not being read at the hearing, and taking the judgment without discussing the legality of the data obtained in a clear manner as sufficient grounds for reversal³²⁵. Moreover, misuse of these measures can amount to “Crimes against Private Life and Confidentiality of Life” as punished under the TCL and criminal liability of officers who take part in the application of the measure can be evoked.

The TCPL also allows defendants to challenge the decisions related to the measures rendered by the Court, judge or in certain cases by prosecutors within the period of seven days starting from the notification of the decision³²⁶. If there is any material or moral damages arising from one of the applied measure listed under Article 141 TCPL, individuals may claim all kinds of material and moral damages³²⁷. Another available judicial redress mechanism is the complaint mechanism described above for measures of public authorities that can be used by suspects or defendants who are subject to the one of the aforementioned measures to claim a violation of their rights guaranteed under the ECHR. In compliance with Turkish Law, the mentioned safeguards apply to all individuals, including foreigners, before the courts without any specific limitation.

2.2.3 DATA SUBJECT RIGHTS

The Turkish Constitution recognises that the right to data protection includes the following data subjects’ rights: (i) right to be informed, (ii) right of access, (iii) right of rectification and deletion and (iv) right to know whether his or her data is processed in line with the specified purpose. The Constitutional Court

³²² Strong suspicion means that when there is a strong probability of conviction at the end of the judgement to be made according to the available evidence.

³²³ See, AYM, E.2018/137, K.2022/86, 30/06/2022, paragraphs 346-368, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/86>.

³²⁴ This is also guaranteed by Article 38(6) of the Constitution: “*Findings obtained through illegal methods shall not be considered evidence.*”

³²⁵ See also decision from the Court of Cassation Yargıtay Yargıtay Ceza Genel Kurulu, 17.02.2006, 2006/5 E, 2006/180 K; Yargıtay Ceza Genel Kurulu 04.07.2006, E. 2006/5-127, K. 2006/180; Yargıtay Ceza Genel Kurulu, 14.10.2008, E.2008/8-49, K. 2008/219.

³²⁶ Article 268/3 CPL.

³²⁷ See the broad interpretation of the Article 141 TCPL by the Court of Cassation; see AYM, İlhan Gökhān, B. No: 2017/27957, 9/9/2020, paragraphs 24-27, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/27957>.

referred to these rights while determining the scope of right to personal data protection in its case law³²⁸. The Court explicitly stated that the right to personal data in Article 20 of the Constitution included these data subject rights and any interference with these rights needed to respect the constitutional protection³²⁹. The importance of recognising these rights at the constitutional level is that if individuals are not satisfied with the data subject rights given to them in the secondary legislation or in practice, they can make an individual complaint before the Constitutional Court.

Despite the fact that these rights are recognised at the constitutional level, the exercise of these rights is to be further defined in secondary legislation, including by setting the conditions to use them. For instance, the TPDPL recognises these rights. However, individuals cannot exercise the data subject rights recognised under the TPDPL when personal data are processed either for intelligence, crime prevention or crime investigation and prosecution purposes. This is because the processing of personal data for intelligence activities, criminal investigation as well as prosecution are excluded from the TPDPL according to Article 28(1)(ç). Indeed, it can be argued that individuals can exercise the right of access and the right to be informed in relation to private entities in accordance with Article 11(ç) under the TPDPL for the government access for intelligence purposes. However, due to the sensitive nature of data access for intelligence purposes, private entities may not disclose the scope of access because doing so could result in the disclosure of intelligence information or operations in general, which could jeopardise intelligence activities carried out by intelligence organisations.

The right to obtain information in the Constitution can be considered as a way of exercising the right of access in the absence of data subject rights. This right is recognised in Article 74(4) of the Constitution as well as in the Law on the Right to Information, dated 2003 and numbered 4982³³⁰. Similarly, the Constitutional Court in a judgment of January 2023, considered this right of information as a data subject access right, which is recognised in Article 20 of the Constitution for individuals³³¹. The Constitution recognises this right for everyone and Article 4(1) of the Law on Right to Information reiterates this. However, Article 4(2) states that only foreigners domiciled in Türkiye, subject to the principle of reciprocity, can exercise the right to information. Thus, it seems that this right cannot be exercised by foreigners residing outside of Türkiye if Article 4(2) is interpreted restrictively. However, as the Constitution recognises this right to everyone without any limitations, this type of interpretation can be considered incompatible with Article 74(4) of the Constitution. Therefore, it can be argued that foreigners residing outside Türkiye can also exercise this right.

While the right to obtain information from intelligence entities or judicial entities is limited, they are not fully excluded from its scope. For the information processed in the context of judicial investigations or prosecutions (Article 20), access requests will not be met if the disclosure prejudices the criminal investigation. It is not possible to initiate an access request for information or documents concerning state intelligence, unless they affect the professional honour and working life of the person according to Article 18(2) of the Law on Right to Information. As the professional honour and working life of the person is not defined in this law, the ordinary meaning of the term has to be considered relevant. In particular, if any intelligence provided by the MIT leads a public entity to not assign a person to a specific role within the state might affect the professional life of a person.

Access requests by individuals are further restricted by an additional paragraph added to Article 30 of the MIT Law³³². According to Article 30(5) of the MIT Law, the MIT is fully excluded from the scope

³²⁸ One of the interviewees refers to one of the latest cases in relation to the data subject rights, see AYM, *Ümit Eyiipoğlu*, B. No: 2018/6161, 28/6/2022, paragraph 18, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/6161>.

³²⁹ Ibid, paragraph 48.

³³⁰ The purpose of the law according to Article 1 is to exercise the right of individuals to obtain information in accordance with the principles of equality, impartiality and openness, which are the requirements of democratic and transparent administration, available at: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4982.pdf>.

³³¹ AYM, E.2018/137, K.2022/86, 30/06/2022, paragraph 134, available at:

<https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2022-86-nrm.pdf>.

³³² One of the interviewees mentions this new exclusion and refers to this new case, AYM, E.2018/137, K.2022/86, 30/06/2022, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/86>.

of Law on the Right to Information. However, the Constitutional Court, in its decision numbered 2022/86, which was published on 12 January 2023, found this additional paragraph (Article 30(5) of the MIT Law) incompatible with Article 20 (right to data protection) and Article 74 (right to obtain information) of the Constitution³³³. In its reasoning, the Court stated that it is possible that some of the information and documents to which the rule prohibits access are personal data. The Court stated that excluding the possibility of accessing documents and information related to his/her social life by individuals prevent its correction and deletion, thus, it constitutes an interference with the right to personal data³³⁴. The Court underlined the importance of access to personal data for preventing arbitrary practices in the democratic and transparent exercise of public power³³⁵. While the Court found that the interference is restricted by law and pursues a legitimate interest, the complete exclusion of MIT from the scope of right of access cannot be considered as proportionate³³⁶. The Constitutional Court stated that personal data access is possible within the defined scope under the Law on Right to Information. Therefore, individuals may exercise the right to obtain information about their personal data processing as long as the information affects their professional honour and working life.

There is no possibility for individuals to obtain confirmation of the legality of data processing by an administrative independent authority. However, if the access to information request is not fulfilled at all or individuals consider that the information processed is illegally obtained, the response to the request can be considered as an administrative action, and they can initiate the annulment action, which has been discussed above in section 2.2.2.1, regarding the decision by the MIT before the administrative courts.

Moreover, in the context of criminal investigations and prosecutions, within the framework of Article 153 TCPL, the defence counsel of the suspect has the right to examine the case file and can access the information gathered through these measures. This can be considered as a way of exercising a right of access.

2.2.4 OVERVIEW OF RELEVANT LEGISLATION

Public authority activity	Laws applied	Oversight	Redress mechanisms
National Security	MIT Law	Parliament Oversight Ombudsman State Council Ex-ante judiciary review for certain measures (access to metadata and content data for the citizens living inside Türkiye)	Judiciary
National Security, Crime Prevention	Police Law Gendarmerie Law	Parliament Oversight Ombudsman State Council Ex-ante judiciary review for accessing to the metadata and content data of communications	Judiciary
Crime Investigation and Prosecution	TCPL	Ex-ante judiciary review for the computer seizure and	Judiciary

³³³ Ibid, paragraph 188.

³³⁴ Ibid, paragraph 174.

³³⁵ Ibid, paragraph 188.

³³⁶ Ibid.

		interception of correspondence through telecommunication	
--	--	----------------------------------------------------------	--

3 CONCLUSION

This study has assessed the relevant legal frameworks and practices around governmental access for the countries of Mexico and Türkiye. The paragraphs below summarise the main findings of the report for each of the assessed jurisdiction.

Mexico has a robust legal system for data protection, with the constitutional text protecting not only the right to data protection but also the ARCO rights (access, rectification, cancelation, and objection). This guarantees that data protection rights are applied to any person, regardless of their nationality, having access to the whole National Transparency System. The protection of personal data is mainly ensured by two general laws: one focused on the private sector (LGPDSSP) and one on the public sector (LGPDSSO). Both laws serve as a general parameter that must be implemented in all the different jurisdictions of the Mexican federation. Thus, the decentralised system leads to the existence of different data protection authorities, also responsible for overseeing the transparency rules. The INAI has a crucial role in overseeing the regional authorities while working side by side with federal authorities. The INAI competences also complement the role of judicial authorities in overseeing surveillance measures.

Governmental access for the purpose of national security is outside the scope of these general data protection laws. These activities should observe the National Security Law (NSL), which also foresees different mechanisms to guarantee the principle of data minimisation and information security. However, data processing for national security reasons lacks any details on the oversight of these activities. Considering that national security is an exception for the data protection laws, there is uncertainty on the extent to which the competent data protection authorities can act on these matters. The main challenges therefore seem to be related to the establishment of a structured oversight system. Reported difficulties also include the guaranteeing of a harmonised application of the different levels of norms, ensuring the independence of the existing authorities, and resisting political interference with such authorities. Upcoming legal initiatives should not undermine the already existing safeguards and rights, but further a proportional approach to develop security and privacy.

Türkiye has a strong constitutional protection for personal data protection. Article 20 of the Turkish Constitution explicitly recognises personal data protection as a fundamental right in addition to right to privacy. This right is granted to everyone including foreigners and includes a right to be informed, a right of access, a right to rectification, and a right to be forgotten. Despite the broad protection given at the constitutional level, the TPDPL, which ensures personal data protection at the secondary level, excludes the processing of personal data by judicial authorities, law enforcement and intelligence organisations. This exclusion of the data processing activities by intelligence and law enforcement authorities from the TPDPL does not mean that these organisations can process personal data arbitrarily. Considering the respective safeguards and oversight mechanisms, the Constitutional Court stated that the exclusion of the data processing activities by these organisations from the TPDPL is necessary and proportionate. Moreover, as confirmed during interviews, several amendments to the TPDPL are expected to be introduced in 2023 in order to align with the GDPR rules, although the details of the amendments are not yet clear or accessible. Individuals regardless of whether they are residing in Türkiye can seek ex-post judicial redress. Furthermore, they can initiate individual complaints of violation of the right to privacy and the right to data protection before the Turkish Constitutional Court after exhausting possible legal remedies. If individuals are not satisfied with the decision of the Constitutional Court, they can claim a violation of their rights guaranteed under the ECHR before the ECtHR.

Yet, the proportionality of government data access is questionable in four regards. First, the substantial and procedural conditions for the government data access for intelligence purposes, lack reference to the requirements of proportionality and necessity of the measure. Second, as it is raised in the dissenting opinion of the Constitutional Court in the case on the MIT Law, lowering safeguards for citizens living abroad and foreigners might not be justified without imposing further substantial and procedural

conditions, which substantiates the notion of necessity and proportionality. Third, despite the fact that three ex-post judicial redress mechanisms are available, other oversight mechanisms (parliamentary oversight, DDK's oversight and Ombudsman's oversight) are limited since they are not specifically designed for an independent oversight of data processing activities for these purposes. Fourth, despite the recognition of the data subject rights at the constitutional level, the rights are not further recognised in the legislation except for a limited right to information and a right of access. However, this does not prevent individuals from invoking the constitutional data subject rights. If public entities do not respond to these rights' requests or individuals are not satisfied with the responses, individuals can invoke these rights before the Constitutional Court after exhausting legal remedies.

ANNEX 1 – QUESTIONNAIRES

Mexico

General questions

1. Both the Law on the Protection of Personal Data in the Possession of Private Parties (LFPDPPP) and the Law on the Protection of Personal Data in possession of Public Parties (LGPDPPSO) foresee different rights for the data subjects. Are data subjects finding more difficulties in exercising their rights in one of the systems when compared to the other?
2. Do the provisions in data protection law (specially the LGPDPPSO) that foresee that every person has the right to data protection guarantees mean that foreigners, including EU citizens, residing inside or outside of Mexico can exercise their rights to guarantee the protection of their personal data?
3. Touristic areas have adopted various surveillance technologies because of the rise of security concerns. In this matter, the National Commission of Human Rights has published a recommendation highlighting the lack of regulation of the use of these technologies. Are there any existing bills about the regulation on how surveillance technologies should or can be used by public authorities in public spaces? What are the current policies and legal developments in this area?
4. Considering the Mexican open data initiative, is there any evidence of inaccuracy or negative effects regarding the information published/made available?
5. What are the legal safeguards regarding data sharing between public authorities also considering the open data initiative adopted in Mexico and the Law on the Protection of Personal Data in the possession of Public Parties (LGPDPPSO)? What are the main risks foreseen for public initiatives that rely on data sharing between public authorities (e.g., national ID card scheme)?
6. Are there any restrictions on data subjects' rights when the purpose of the processing of data is intelligence or national security?
7. Are there any ongoing legislative or policy developments that address the use of technology by third countries such as the US that directly affect data subjects in Mexico (e.g., use of facial recognition by the US government in the borders with Mexico)?
8. What are the regulations on data sharing from one Mexican public authority to another (onward sharing)? How do the data subject rights apply in these situations?
9. What are the existing rules regarding data transfers from Mexico to other (third) countries, especially when the personal data was collected or accessed by a Mexican public authority?

Data subject rights and legal remedies

10. What are the enforcement powers of INAI (Federal Institute for Access to Public Information and Data Protection) when it comes to criminal procedures or national security law? How do these provisions apply in cases of interception of private communications?
11. What is INAI's role in overseeing regional activities regarding the processing of data by local public authorities? Does this also apply to the evaluation of Data Protection Impact

Assessments (*Evaluaciones de Impacto en la Protección de Datos Personales*)? Do public authorities have to prove the security of the systems used by them in data processing activities?

12. What mechanisms does INAI have to report infringements of the law to judicial courts (Article 89 of the LGPDPPSO)?
13. Are the guidelines and recommendations published by INAI used by judicial courts in decisions regarding data protection?
14. The General Law for Transparency obliges authorities involved in communication surveillance to publish periodic reports, including the judicial authorisations that led to the surveillance measure (e.g., Article 18). However, the telecommunications' regulators removed the transparency obligations foreseen in the previous Guidelines for Collaboration on Security and Justice Matters. How is this system currently working? Are there any obligations regarding this topic?
15. Does the legal system determine when the data subject should be notified after she/he was targeted with a surveillance mechanism (e.g., intercept of private communications)? Are there any legal provisions on how and when the unnecessary data should be deleted?
16. Article 68, III, of the General Law for Transparency, foresees the obligation of informing data subjects about aspects of the processing of personal data, but this obligation does not apply when the public authorities are acting within their legal attributions. In this scenario, how does the principle of transparency apply?
17. Considering the recent decisions of the Supreme Court of Justice, what are the existing mechanisms to modify a decision published by INAI?

Türkiye

General Questions

1. What is your opinion on government data access in Türkiye and existing data protection safeguards for data subjects? (Please consider the broad exceptions for data processing for law enforcement and intelligence purposes in Türkiye.)
2. How is personal data protected while there's no specific law about processing for criminal prosecution, national defence and security or public safety?
3. What are the legal protection mechanisms provided to foreigners, including EU citizens, residing outside Türkiye in case of processing their data for law enforcement purposes as well as intelligence purposes? (Please consider legal remedies such as at courts, complaint mechanisms at the authorities themselves, or at a supervisory authority.)
4. Do foreigners, including EU Citizens, have equivalent protection of their fundamental rights when their personal data are processed for law enforcement purposes and in case of government access to data? (Please compare with data subjects residing in Türkiye.)
5. What are the legal rules on data transfers from Türkiye to other countries, especially for governmental authorities who might have previously received that data via governmental access?

Data Subject Rights and Legal Remedies

6. Do data subjects have any rights and safeguards (e.g., legal remedies to invoke at court or a public authority to gain access, rectification or erasure) when their personal data are processed for law enforcement and intelligence purposes? If so, what are the limitations? (e.g., considering the data protection law, criminal procedural law, right to information, constitutional law etc.)
7. What do you think about the feasibility of invoking the right to information (e.g., Presidency's Communication Centre etc.) as a data access right in case of processing personal data by law enforcement and intelligence services?
8. As a follow-up to question 5, what do you think about the available rights and safeguards in case of unlawful processing of personal data by law enforcement authorities or intelligence services (i.e., administrative law, criminal law, constitutional law)?
9. As a follow-up to question 5, are there any limits to these rights and safeguards specific to the case of a foreign data subject, including EU citizens, who wants to rely on them, residing outside Türkiye?

Possible objection mechanisms to government access request

10. If a government access request is made to economic operators (e.g., Internet service providers, telecommunication providers) in Türkiye, what are the processes that need to be carried out to fulfil this request? (Please answer the question considering the different applicable regimes to requests by law enforcement and intelligence agencies.)
11. Are there any legal objection mechanisms provided to economic operators against the request made by the requesting government authorities?
 - a. If the answer is yes to question 11, how does it occur in practice?

- b. If the answer is no to question 11, is there any possibility of informing data subjects about government data access?

Upcoming legal initiatives

12. Are there any upcoming policy or legal initiatives concerning data protection and government access to personal data in Türkiye? (Please consider the scope and adequacy of the proposed amendments to the data protection law.)

ANNEX 2 – SOURCES OF INFORMATION

General Part

Case law

CJEU

- Judgment of the Court (Grand Chamber) of 20 September 2022, C-339/20 VD and C-397/20 SR, ECLI:EU:C:2022:703.
- Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D v The Commissioner of the Garda Síochána, and Others*, C-140/20, ECLI:EU:C:2022:258.
- Judgment of the Court (Tenth Chamber) of 21 October 2021, *the Spetsializiran nakazatelen sad*, C-350/21, ECLI:EU:C:2021:874.
- Judgment of the Court (Eighth Chamber) of 2 September 2021, *Telekom Deutschland GmbH v Bundesrepublik Deutschland*, C-794/19.
- Judgment of the Court (Grand Chamber) of 22 June 2021, *Ordre des barreaux francophones et germanophone and others*, C-512/18, ECLI:EU:C:2021:505.
- Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, ECLI:EU:C:2021:152.
- Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.
- Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18, ECLI:EU:C:2020:791.
- Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, ECLI:EU:C:2020:559.
- Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.
- Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14 ECLI:EU:C:2015:650.
- Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.
- Judgment of the Court (Fourth Chamber) of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670.
- Judgment of the Court (Grand Chamber), 26 February 2013, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2013:107.
- Judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727.
- Judgment of the Court of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596.
- Judgment of the Court (Grand Chamber) of 20 September 2022, *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH.SpaceNet*, C-793/19, ECLI:EU:C:2022:702.

ECtHR

- Judgement of 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013.
- Judgement of 4 December 2015, *Zakharov v. Russia*, no. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306.
- Judgement of 18 May 2010, *Kennedy v. the United Kingdom*, no. 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905.
- Judgement of 2 December 2008, *K.U. v. Finland*, no. 2872/02, ECLI:CE:ECHR:2008:1202JUD000287202.
- Judgement of 29 June 2006, *Weber and Saravia*, no. 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400.

Judgement of 4 March 2004, <i>M.C. v. Bulgaria</i> , no. 39272/98, ECLI:CE:ECHR:2003:1204JUD003927298.
Judgement of 4 May 2000, <i>Rotaru v. Romania</i> , no. 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195.
Judgement of 16 February 2000, <i>Amann v. Switzerland</i> , no. 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895.
Judgement of 28 October 1998, <i>Osman v. United Kingdom</i> , no. 23452/94, ECLI:CE:ECHR:1998:1028JUD002345294.
Judgement of 24 April 1990, <i>Huvig v. France</i> , no. 11105/84.
Judgement of 26 March 1987, <i>Leanderv. Sweden</i> , no. 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881.
Judgement of 2 August 1984, <i>Malone v. the UK</i> , no. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179.
Judgement of 26 April 1979, <i>The Sunday Times v. the UK</i> , no. 6538/74, ECLI:CE:ECHR:1979:0426JUD000653874.

Opinions

Opinion of the Court (Grand Chamber) of 26 July 2017, Opinion 1/15 on the EU-Canada PNR Agreement, ECLI:EU:C:2017:592.

Other sources

- European Data Protection Board (2023), *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.
- European Data Protection Board (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*.
- European Data Protection Board (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*.
- European Data Protection Supervisor (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*.
- European Data Protection Supervisor (2021), *Case Law Digest: Transfers of personal data to third countries*.
- European Data Protection Supervisor (2019), *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*.
- European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018.
- Gerards, J., ‘How to improve the necessity test of the European Court of Human Rights’, *International Journal of Constitutional Law*, Vol. 11, No 2, April 2013, pp. 466–490.
- Lenaerts, K., ‘Limits on Limitations: The Essence of Fundamental Rights in the EU’, *German Law Journal*, Vol. 20, pp. 779-793, Cambridge University Press, 2019.
- Brkan, M., ‘The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU’s constitutional reasoning’, *German Law Journal*, Vol. 20, pp. 864-883, Cambridge University Press, 2019.
- Tridimas, T., Gentile, G., ‘The essence of Rights: An Unreliable Boundary?’, *German Law Journal*, Vol. 20, pp. 794–816, Cambridge University Press, 2019.
- Tracol, X., ‘Ministerio fiscal: Access of public authorities to personal data retained by providers of electronic communications services’, *European Data Protection Law Review*, Vol. 5, No 1, pp. 127-135.

Mexico

Case law

- Supreme Court of Justice (*Suprema Corte de Justicia*), *Amparo Directo en Revisión* 6489/2018.
- Supreme Court of Justice (*Suprema Corte de Justicia*), Case n. 2005522, Thesis P. II/2014, January 21st of 2014.
- Supreme Court of Justice (*Suprema Corte de Justicia*), Case n. 2011608, Thesis 2a. XIX/2016 (10a), May 2016.
- Supreme Court of Justice (*Suprema Corte de Justicia*), Case n. 2018460, Thesis I.10o.A.70 A (10a), November 2018.
- Supreme Court of Justice (*Suprema Corte de Justicia*), Case n. 2024641, Thesis 2a./J. 23.2022 (11a), May 2022
- Supreme Court of Justice (*Suprema Corte de Justicia*), *Controversia Constitucional*, P.J. 136/2005.

Legislation

- Congreso General de los Estados Unidos Mexicanos, *Código Nacional de Procedimientos Penales*, March 2014, available at: <https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf>.
- Congreso General de los Estados Unidos Mexicanos, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, July 2010, Spanish text available at: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.
- Congreso General de los Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, January 2017, Spanish text available at: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPSSO.pdf>.
- Congreso General de los Estados Unidos Mexicanos, *Ley General de Transparencia y Acceso a la Información Pública*, May 2015, Spanish text available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP_200521.pdf.
- Congreso de los Estados Unidos Mexicanos, *Ley de Seguridad Nacional*, January 2005, Spanish text available at: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf>.
- Mexico, *Constitución Política de los Estados Unidos Mexicanos*, 1917, English version available at: https://www.constituteproject.org/constitution/Mexico_2015.pdf?lang=en.

Other sources

- Article 19 (2022), *Mexico: Article 19 condemns continued assault on its work and the press*, Press release, available at: https://www.article19.org/wp-content/uploads/2022/12/article19_2022_comunicado_ingles.pdf.
- CNI, *Aviso de Privacidad Integral*, available at: <http://www.cni.gob.mx/transparencia/docs/Aviso-Privacidad-Integral.pdf>.
- CNI, *Guía para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales*, available at: <http://www.cni.gob.mx/transparencia/docs/Guia-ARCO.pdf>.
- Estado de México, *Periódico Oficial Gaceta del Gobierno y LEGISTEL, Leyes Nacionales, Generales y Federales*, available at: https://legislacion.edomex.gob.mx/leyes_federales.
- Estrada, J. M. M. (2015), *Configuración normativa de las leyes en el marco competencial de los órdenes jurídicos, Congreso Redipal Virtual VIII*, available at: <https://www.diputados.gob.mx/sedia/sia/redipal/CRV-VIII-14-%2015.pdf>.
- García, A. G. (2016), *Transparency in Mexico: An Overview of Access to Information Regulations and their Effectiveness at the Federal and State Level*, Report, Wilson Center Mexico Institute.
- Human Rights Watch (2019), *México: La transparencia y la privacidad, amenazadas*, available at: <https://www.hrw.org/es/news/2021/01/28/mexico-la-transparencia-y-la-privacidad-amenazadas>.
- INAI, *El ABC del aviso de privacidad. Sector Público*, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_ABC-AP-SPublico.pdf.
- INAI, *Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf.
- INAI (2022), *Informe de Labores 2022*, available at: <https://micrositios.inai.org.mx/informesinai/>.

- INAI (2022), *Recomendaciones para los sujetos obligados en las comunicaciones de datos personales*, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones-SO_Comun_DP.pdf.
- Lopes, T. M. G., ‘Las recientes reformas em materia de protección de datos personales em México’, *Anuario Jurídico y Económico Escurialense*, XLIV, 2011, pp. 317-334, ISSN: 1133-3677.
- López, L. C. J., ‘Seguridad nactional, inteligencia militar y acceso a la información en México’, *URVIO Revista Latinoamericana de Estudios de Seguridad*, No 21, 2017, available at: http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-42992017000100140&script=sci_arttext.
- López, S. T., ‘Sustitución de la Ley Federal de Archivos de México: el alcance de una ley general’, *Revista Española de la Transparencia*, No 12, January - June 2021, pp. 167-187.
- Mexico, Senado de la República, *Código Nacional de Procedimientos Penales*, 2014, available at: senado.gob.mx/comisiones/justicia/docs/CNPP.pdf
- Mexico, *Lineamientos Generales de Protección de Datos Personales para el Sector Público*, 2017, available at: https://www.gob.mx/cms/uploads/attachment/file/304930/lineamientos_generales_para_la_protección_de_datos_personales_para_el_sector_p_blico.pdf.
- OECD (2022), *Declaration on Government Access to Personal Data Held by Private Sector Entities*, available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

Türkiye

Case Law

Judgment of the European Court of Human Rights 6 September 1978, *Klass and ors v Federal Republic of Germany*, no. 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978).

AYM, *Bestami Eroğlu [GK]*, B. No: 2018/23077, T. 17/9/2020, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/23077?BasvuruAdi=BESTAM%C4%B0+ER%C4%9ELU>.

AYM, E.2019/96, K.2022/17, T. 24/02/2022, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/17>.

AYM, E.2018/137, K.2022/86, 30/06/2022, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/86>.

AYM E.2016/125., K.2017/143, 28/09/2017, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/143?KararNo=2017%2F143>.

AYM, E.2014/122, K.2015/123 T. 30/12/2015, available at: <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123>.

AYM, *Ercan Kanar*, B. No: 2013/533, 9/1/2014 available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/533>.

AYM, *İlhan Gökhan*, B. No: 2017/27957, 9/9/2020, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/27957>.

AYM, *Ümit Eyüpoglu*, B. No: 2018/6161, 28/6/2022, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/6161>.

AYM, *Yasemin Çongar ve diğerleri [GK]*, B. No: 2013/7054, 6/1/2015, available at: <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/7054>.

The Ombudsman Institution, Application No. 2019 4234, 23 August 2019, available at: <https://kararlar.ombudsman.gov.tr/Arama/Download?url=20190219\19438\Yayin\Karar-2019-4234.pdf&tarih=2019-08-23T14:09:55.848612>.

Legislation

The Administrative Procedure Law of Türkiye, numbered 2577 and dated 1982, available at: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2577.pdf> <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2577.pdf>.

The Constitution of the Republic of Türkiye provided by Grand National Assembly of Türkiye, GNAT, May 2019, available at: https://www5.tbmm.gov.tr/yayinlar/2021/TC_Anayasasi_ve_TBMM_Ic_Tuzugu_Ingilizce.pdf.

The Law on the Duties and Powers of the Gendarmerie Organization, dated 1983 and numbered 2803 (Gendarmerie Law), available at: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2803.pdf>.

The Law on the Duties and Powers of Police, dated 1934 and numbered 2559 (Police Law), available at: <https://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf>.

The Law on the Ombudsman Institution, numbered No.6328 and dated 2012, available at: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6328.pdf>.

The Law on the Right to Information, dated 2003 and numbered 4982, available at: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4982.pdf>.

The Law on the State Intelligence Services and the National Intelligence Organisation, numbered 2937 and dated 1983 (MIT Law), available at: <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2937&MevzuatTur=1&MevzuatTertip=5>.

The Presidential Decree on Devlet Denetleme Kurulu, available at: <https://www.mevzuat.gov.tr/MevzuatMetin/19.5.5.pdf>.

The Regulation on Procedures and Principles Relating to Authorization to Access Providers and Hosting Providers, available at: <https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=7&MevzuatNo=11679&MevzuatTertip=5>.

Turkish Personal Data Protection Law, numbered 6698 and dated 2016, available at: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf>,

Other sources

- Akman, N. G. (2021), *Protection of Personal Data by Administrative Law* (Master Thesis), available at: https://tez.yok.gov.tr/UluselTezMerkezi/TezGoster?key=v7BkNnepTnbhn8rNR77LcR_II-f_TK_3XoNmW2wSHu86pEYn4zgNqFITXoQxtnR.
- Alyanak, S., *The New Institution on Protection of Fundamental Rights: Turkish Ombudsman Institution*, available at: <https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/42699>.
- Atlı, T. (2019), 'KİŞİSEL VERİLERİN ÖNLEYİCİ, KORUYUCU VE İSTİHBARI FAALİYETLER AMACIYLA İŞLENMESİ', 2 Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, available at: <https://dergipark.org.tr/tr/download/article-file/747023>.
- Council of Europe, *European Court of Human Rights, Annual Report 2022*, available at: https://www.echr.coe.int/Documents/Annual_report_2022_ENG.pdf.
- Council of Europe, *Interim Resolution on Execution of the judgment of the European Court of Human Rights Kavala against Turkey*, available at: <https://rm.coe.int/0900001680a4b3d4>.
- Council of Europe, *Violations by Article and by State*, available at: https://www.echr.coe.int/Documents/StatsViolation_1959_2022_ENG.pdf.
- Council of Europe Committee on Counter-Terrorism (CDCT), *Profiles on Counter-Terrorism Capacity: Türkiye*, available at: <https://rm.coe.int/profile-november-2022-Türkiye/1680a94979>.
- Erhan, Z. (2019), *Core International Crimes In Turkish Criminal Law And The Rome Statute*, 22 Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, p. 111.
- European Commission, *Türkiye 2022 Report*, available at <https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf>.
- European Commission for Democracy Through Law (Venice Commission), *Draft Opinion on the Provisions of the Emergency Decree Law N° 674 of 1 September 2016 which Concern the Exercise of Local Democracy in Türkiye*, available at: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2017\)021-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2017)021-e).
- Human Rights Action Plan (2021-2023), Circular 2021/9, available at: https://insanhaklarieylemplani.adalet.gov.tr/resimler/%C4%B0nsan_Haklar%C4%B1_Eylem_Pl%C4%B1_ve_Uygulama_Takvimi.pdf.
- Human Rights Watch, *Council of Europe Sanctions Turkey*, available at: <https://www.hrw.org/news/2021/12/03/council-europe-sanctions-Türkiye>.
- Human Rights Watch, *Türkiye Spy Agency Law Opens Door to Abuse*, available at: [https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse#:~:text=\(Istanbul\)%20E2%80%93%20A%20new%20law,an%20the%20right%20to%20privacy](https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse#:~:text=(Istanbul)%20E2%80%93%20A%20new%20law,an%20the%20right%20to%20privacy).
- Human Rights Watch, *Turkey: YouTube Precedent Threatens Free Expression*, available at: <https://www.hrw.org/news/2020/12/19/turkey-youtube-precedent-threatens-free-expression>.
- Kaya, M. B., Tastan, F., *Kişisel Veri Koruma Hukuku: Mevzuat & İctihat & Bibliyografya*, online, version 2.5, pp. 1774-1776, available at: <https://mbkaya.com/kisisel-veri-koruma-hukuku-mevzuat-ictihat/>.
- Medyascope, *BTK-gate: Internet activity, identity, and personal data of all users in Turkey has been collected by BTK for the past year and a half*, available at: <https://medyascope.tv/2022/07/21/btk-gate-internet-activity-identity-and-personal-data-of-all-users-in-Türkiye-has-been-collected-by-btk-for-the-past-year-and-a-half/>.
- OECD, *Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access*, available at: <https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm#>.
- Olgunsoy, F. (2019), *The Impact of Intelligence Activities in Fight Against Terror on Liberties: Turkey, United Kingdom, United States of America* (PhD Thesis), available at: <http://nek.istanbul.edu.tr:4444/ekos/TEZ/60634.pdf>.
- Personal Data Protection Supervisory Authority of Türkiye, *Bağlayıcı Şirket Kuralları Hakkında Kamuoyu Duyurusu*, 10 April 2020, available at: <https://www.kvkk.gov.tr/Icerik/6728/YURT>.

DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU.

Personal Data Protection Supervisory Authority of Türkiye, *International Data Transfer*, available at:
<https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim>,
<https://www.kvkk.gov.tr/Icerik/4106/Kisisel-Verilerin-Yurtdisina-Aktarilmasi>.

Personal Data Protection Supervisory Authority of Türkiye, *Yurtdisina Veri Aktariminda Veri Sorumlularinca Hazirlanacak Taahhutnamede Yer Alacak Asgari Unsurlar*, 2018, available at:
<https://kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-VeriSorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-AsgariUnsurlar>.

Personal Data Protection Supervisory Authority of Türkiye, *5. yılında Kişisel Verileri Koruma Kurumu*, 23 November 2022, available at: <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/b5731c6c-540b-45eb-a2d8-d7cef57cf197.pdf>.

Ünver, H. A., Kim, G., ‘Data Privacy and Surveillance in Türkiye’, *EDAM Cyber Policy Paper Series* 2, 13 February 2017.

ANNEX 3 – ACRONYMS AND ABBREVIATIONS

General

Acronyms and Abbreviations	Meaning
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Convention 108+	Convention 108+ on protection of individuals with regard to the Processing of Personal Data
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
EU-Charter	Charter of Fundamental Rights of the European Union
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
HRC	United Nations Human Rights Council
HRW	Human Rights Watch
ICCPR	International Covenant on Civil and Political Rights
OECD	Organisation for Economic Co-operation and Development
SA(s)	Supervisory authority(-ies)
UDHR	Universal Declaration of Human Rights
UN	United Nations

Mexico

Acronyms and Abbreviations	Meaning
Constitution	Constitución Política de los Estados Unidos Mexicanos
ARCO	Right to access, correction, cancelation and opposition (<i>derechos de acceso, rectificación, cancelación u oposición</i>)
CNPP	Criminal Procedure Code (<i>Código Nacional de Procedimientos Penales, de 5 de marzo de 2014</i>)
INAI	National Institute for Transparency, Access to Information and Data Protection
LFPDSSPP	Data Protection Law for Private Parties (<i>Ley Federal de Protección de Datos Personales en Posesión de los Particulares</i>)
LGPDSO	Data Protection Law for Public Parties (<i>Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados</i>)
LFTAIP	Federal Law of Transparency and Access to Public Information (<i>Ley Federal de Transparencia y Acceso a la Información Pública</i>)
LGTAIP	General Law of Transparency and Access to Public Information (<i>Ley General de Transparencia y Acceso a la Información Pública</i>)
NSL	National Security Law (<i>Ley de Seguridad Nacional, de 31 de enero de 2005</i>)

Türkiye

Acronyms and Abbreviations	Meaning
Constitution	The Constitution of the Republic of Türkiye
EU	European Union
CoE	Council of Europe
ECHR	European Convention of Human Rights
GNAT	Grand National Assembly of Türkiye
GDPR	General Data Protection Regulation
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
OECD	Organisation for Economic Co-operation and Development
ECtHR	European Court of Human Rights
HRW	Human Rights Watch
BTK (ICTA)	Bilgi Teknolojileri ve İletişim Kurumu (Information and Communication Technologies Authority)
TCL	Turkish Criminal Law
TPDPL	Turkish Personal Data Protection Law
SA	Personal Data Protection Supervisory Authority of Türkiye
the Board	Personal Data Protection Board
SCCs	Standard Contractual Clauses
BCR	Binding Corporate Rules
MIT	Milli İstihbarat Teşkilatı(National Intelligence Organization)
MIT Law	Law numbered 2937 on the State Intelligence Services and the National Intelligence Organization
DDK	Devlet Denetleme Kurulu(the State Supervisory Council)
TCPL	Turkish Criminal Procedure Law
AYM	Türkiye Cumhuriyeti Anayasa Mahkemesi(The Constitutional Court of Türkiye)
HTS	Historical Traffic Search

Note



1st meeting of the Coordinated Supervision Committee

3 December 2019, Brussels

Summary

The Coordinated Supervision Committee ("the Committee") met on 3 December 2019 in Brussels.

Information from the Secretariat

The Secretariat provided information on the legal basis of the coordinated supervision referring to Art. 62 of Regulation 2018/1725 and relevant legal basis of the large scale IT systems and EU agencies. The Secretariat informed the Committee members of the indicative calendar for the EDPB to take over the coordinated supervision of EU large scale IT systems and agencies. The Secretariat also presented the draft Rules of Procedure of the Committee, according to which, the work of the Committee will focus on 3 thematic blocks:

- (a) Border, asylum and migration,
- (b) Police and judicial cooperation
- (c) Digital single market.

The approach of having one single committee aims at ensuring a horizontal approach to the coordinated supervision.

Adoption of the Rules of Procedure

The Committee adopted the Rules of Procedure.

Election of the Coordinator

The Committee elected Giuseppe Busia from the Italian supervisory authority as Coordinator and Iris Gnedler from the German Federal supervisory authority as Deputy Coordinator for a term of two years.

IMI

The Committee discussed the implementing legislation to use IMI in new legal areas, the security of the system, and the need to invite the European Commission as the IMI system provider to the next meeting of the Committee.

Note



2nd meeting of the Coordinated Supervision Committee

8 July 2020, Remote

Summary

The Coordinated Supervision Committee ("the Committee") met on 8 July 2020 online.

[Work Program 2020-2022](#)

The Committee discussed its two-year work program for the period July 2020 - July 2022. The Committee members decided to allow for additional time for comments and to submit it for approval via written procedure.

[Eurojust](#)

The Committee received a presentation from the Eurojust DPO on Eurojust's functioning, its legal basis, its processing of personal data and the attribution of responsibilities over it. The Committee discussed the interpretation and application of Article 42 "Cooperation between the EDPS and national supervisory authorities" and a proposal for cooperation between supervisory authorities and law enforcement authorities in cases of data breaches in the area of cybercrime.

[IMI](#)

The Committee received a presentation from the European Commission's DG-GROW on the set-up and processing of data in the EU Internal Market Information (IMI) system. The Committee discussed about how to ensure that data subjects have access to sufficient information on the exercise of their rights with respect to the processing of their personal data in IMI.

[Exercise of data subjects rights in relation to IMI and Eurojust](#)

The Committee decided to focus on examining the exercise of data subjects rights in relation to IMI and Eurojust, paying due consideration to their different nature and characteristics, and the specific issues relevant to systems that process law enforcement and judicial data.

Preparation of supervision of European Public Prosecutor's Office

The Committee discussed its preparation for the planned entry into operation of the European Public Prosecutor's Office (the EPPO) and the need to receive a presentation from an EPPO representative.

Miscellaneous

The next Committee meeting will be held on December 2020.

Note



3rd meeting of the Coordinated Supervision Committee

9 December 2020, Remote

Summary

The Coordinated Supervision Committee (“the Committee”) met on 9 December 2020 online.

[IMI](#)

The Committee discussed the information available to data subjects on the exercise of their rights in relation to the processing of their personal data in IMI at the EU and national level.

A representative from the supervisory authorities’ DPO network explained the network’s ongoing work on examining the processing operations in IMI in relation to the supervisory authorities’ use of IMI for the cooperation and consistency mechanism.

The Committee agreed to prepare a list of data protection supervisory authorities competent in IMI matters and to upload it to the Committee’s public website when it is available.

[Common framework for audits of IMI at the national level](#)

The Committee members discussed the approach to take to prepare a common European-wide framework for audits of IMI conducted at the national level.

[Eurojust related issues](#)

The Committee members discussed the channels national authorities use to communicate and exchange information with Eurojust. The Committee members also discussed Eurojust’s suggestions for cooperation between law enforcement and data protection supervisory authorities in cases of data breaches in the area of cybercrime.

[Large scale IT systems and their interoperability](#)

The Committee members received a presentation from a representative of the EU Agency for Fundamental Rights (FRA) on the FRA’S last research on EU large scale IT systems and their interoperability, with a focus on the EES, ETIAS, and the EU Interoperability Regulations.

Election of a new Coordinator for the CSC

The members of the Committee elected Ms. Clara Guerra, representative of the Portuguese SA, as Coordinator of the Committee, due to the departure of the former Coordinator from the Italian supervisory authority.

Note



4th meeting of the Coordinated Supervision Committee

31 May 2021, Remote

Summary

The Coordinated Supervision Committee (“the Committee”) met on 31 May 2021 online.

IMI

The Committee discussed the preparation of a list of contact details of the competent data protection supervisory authorities on IMI that will be published in the Committee’s section of the EDPB website. The Committee also received from the Secretariat an oral report of aspects of IMI relevant to its supervision and data subject rights, based on the information received from the Committee members. This information will serve for the preparation of a report with recommendations on how to facilitate the exercise by data subject of their rights in relation to the processing of their personal data in IMI.

Eurojust related issues

The Committee discussed some proposals made by Eurojust and Europol on cooperation and exchange of information between supervisory and law enforcement authorities in cases of data breaches in the area of cybercrime. The Committee also received an oral report on the meeting held with Eurojust representatives to obtain information on the Eurojust Counter-Terrorism Register. The Committee examined the secure communication channels used between national authorities and Eurojust to exchange data.

European Public Prosecutor’s Office (EPPO)

The Committee members received presentations from an academic and the EPPO DPO on data protection aspects of the EPPO, which enters into operation on 1 June 2021. The discussions addressed the interplay between the regulations applicable to the EPPO’s processing of data and the controllership over it. The Committee also discussed the next steps to be taken on the supervision of the EPPO at European and national levels.

Organisation of the work of the CSC

The Committee discussed its internal functioning. The Committee also noted the high number of additional EU agencies and information systems that will fall under the CSC’s purview this year and in 2022 and launched its reflection on how to organise its working methods and meetings to cover them effectively.

Note



5th meeting of the Coordinated Supervision Committee

1 December 2021, Remote

Summary

The Coordinated Supervision Committee (the Committee) met on 1 December 2021

IMI

The Committee discussed and adopted a report on the implementation of the Internal Market Information System (IMI) at national level. This report was based on a questionnaire and intended to obtain a general overview of the use of IMI to feed the future work of the CSC. In view of the conclusions taken, the CSC decided to develop recommendations to the national competent authorities, as controllers, regarding GDPR transparency obligations for the IMI data processing. It was agreed to publish the report on the website.

European Public Prosecutor Office (EPPO)

The Committee exchanged information on the state of play of the EPPO start of operation at national level based on an oral report on the first answers received on the EPPO questionnaire and on some updates provided by members during the meeting. It was shared the national legal framework and how the European Delegated Prosecutors (EDPs) have their work environment organised in order to perform their legal tasks, in particular the communication with EPPO and the interaction with other national competent authorities. It was decided to keep following the EPPO's further implementation at Member State level.

Future functioning of the CSC

The Committee discussed and agreed with the proposals presented for the future functioning of the CSC. The Committee will strive to reach a holistic view considering the interaction and interoperability of the European information systems, in order to improve effectiveness in the coordinated supervision activities. The Committee also opted for flexible working methods and will enhance cooperation with external stakeholders.

The Rules of Procedure of the CSC were evaluated. It was consented that no adjustment is needed.

Eurojust audit

The EDPS presented the Eurojust audit that took place on 25-26 October 2021. The audit was based on consultation with the agency. Its scope focussed on the processing of operational data only and on areas subject to legislative changes.

Election of the Deputy Coordinator

The Committee elected Sebastian Hümmeler, from the German Federal Data Protection Authority, as Deputy Coordinator of the CSC, after the term of office of Iris Gnedler came to an end in December.