ANNUAL REPORT 2022

STREAMLINING ENFORCEMENT THROUGH COOPERATION

edpb

European Data Protection Board

European Data Protection Board

An Executive Summary of this report, which provides an overview of key EDPB activities in 2022, is also available. Further details about the EDPB can be found on our website at edpb.europa.eu.

TABLE OF CONTENTS

1

GLOSSARY

Adequacy decision	An implementing act adopted by the European Commission, stating that a non-EU country ensures an adequate level of protection of personal data.
Binding Corporate Rules (BCRs)	Data protection policies adhered to by controllers or processors established in the EU for transfers of personal data to controllers or processors outside the EU within a group of undertakings or enterprises or groups of enterprises engaged in a joint economic activity.
Charter of Fundamental Rights of the EU	A legally binding Charter that sets out the civil, political, economic, social and cultural rights of EU citizens and residents (including the right to the protection of personal data in its Art. 8).
Concerned Supervisory Authorities (CSAs)	A Supervisory Authority concerned by the processing of personal data because: (a) the controller or processor is established on the territory of its Member State; (b) data subjects residing in the Member State are substantially affected by the processing; or (c) a complaint has been lodged with that Supervisory Authority.
Court of Justice of the European Union (CJEU)	The highest court in the EU judiciary system, which ensures uniform interpretation and application of EU law in EU Member States. It ensures those States and EU institutions abide by EU law.
Cross-border processing	Either (a) processing of personal data that takes place in the context of the activities of establishments in more than one Member State due to the controller or processor being established in more than one Member State; or (b) processing of personal data that takes place in the context of the activities of a controller or processor established in a single Member State, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Data controller	The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data minimisation	A principle that means that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Impact Assessment (DPIA)	An impact assessment aiming to evaluate the processing of personal data, including notably a description of the processing and its purposes, an assessment of the necessity and proportionality, an assessment of the risks for the rights and freedom of individuals, and the measures envisaged to address the risks.
Data Protection Officer (DPO)	An expert on data protection, who operates independently within an organisation to ensure the internal application of data protection.
Data subject	The person whose personal data is processed.
European Commission	An EU institution that shapes the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget.
European Economic Area (EEA) Member States	EU Member States and Iceland, Liechtenstein and Norway.
European Union (EU)	An economic and political union between 27 European countries.
General Data Protection Regulation (GDPR)	An EU Regulation that sets out rules on the rights of data subjects, the duties of data controllers and processors processing personal data, international data transfers and the powers of Supervisory Authorities.
Lead Supervisory Authority (LSA)	The Supervisory Authority where the "main establishment" of a data controller or processor is based, which has the primary responsibility for dealing with a cross-border data processing activity and for coordinating any cross-border investigation.

Main establishment	Either (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union; unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; or (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union; or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the GDPR.
One-Stop-Shop mechanism	A mechanism whereby the Supervisory Authority with the "main establishment" of a controller or processor in the EU serves as the Lead Supervisory Authority to ensure cooperation between Supervisory Authorities in the case of cross-border processing.
Personal data	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.
Processing	Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Standard Contractual Clauses (SCCs)	A set of contractual clauses that provide adequate safeguards for data transfers from the EU or the EEA to third countries and govern the relationship between involved controllers and processors.
Supervisory Authority (SA) or Data Protection Authority (DPA)	An independent public supervisory body that monitors the application of the GDPR and other national laws relating to data protection, in order to protect the rights and freedoms of natural persons in relation to the processing of personal data.
Third country	A country outside the EU and EEA.

2

FOREWORD

It is my pleasure to introduce the fifth Annual Report of the European Data Protection Board (EDPB), also the last one published during my mandate as EDPB Chair.

Once again, this Report clearly demonstrates how much work is done by the EDPB in the span of a year, in terms of issuing guidance, consistency documents, legal advice and adopting binding decisions. What is also abundantly clear from this report is how the role of the EDPB has changed.

Today, we are much further than we were in 2018. The GDPR is at the heart of the newly adopted digital single market legislation, which will determine how large online platforms operate in the decades to come. Enforcement of data protection is now making headlines every week. Organisations worldwide are aware they cannot do business in Europe without complying with the GDPR.

Today, the EDPB is a major player in the European Economic Area (EEA) digital economy. It does not just ensure that data protection law is applied consistently across the EEA, but it helps shape Europe's digital future.

On top of being a source of guidance and legal advice, the EDPB has taken a series of important binding decisions in concrete cases in the past year. These decisions have a

far-reaching impact and the potential to change the way large digital players handle our personal data, today and in the future. We thereby help redress a balance that has been tipped too far in favour of large tech companies.

While enforcement has accelerated, there is still a lot we can and are planning to do to make sure the GDPR has the largest impact possible on the protection of people's data protection rights.

In April 2022, EDPB members gathered in my hometown Vienna with a view to finding solutions for more efficient enforcement cooperation. This meeting signalled a commitment of all Data Protection Authorities' (DPA) to deepen cooperation. Numerous initiatives to increase the DPAs' capacity to enforce were agreed upon. We also adopted a list of national administrative procedures that we would like to see streamlined. It is very positive that the European Commission has agreed to take a legislative initiative for greater harmonisation of these procedures, as this will help unlock the GDPR's potential.

It is also important to underline that the depth and breadth of our work could not have materialised without the efforts of everyone involved at the EDPB, and, not in the least, at the EDPB Secretariat. The EDPB Secretariat is a small and very dedicated group of people, without whose efforts and expertise the EDPB would not be able to achieve everything it sets out to do. It is important that we continue to supply the Secretariat with sufficient resources, so that they can provide much needed logistical, administrative and analytical and legal support to the EDPB.

The first five years of the EDPB's existence were the beginning of a process, whereby this new EU body gradually expanded its impact. The next five years will almost certainly bring new challenges, with even more enforcement and, as a result, more litigation too. I am confident that the EDPB will successfully face these new challenges, under the leadership of my successor.

Andrea Jelinek

Chair of the European Data Protection Board

3

2022 – HIGHLIGHTS

3.1. ENFORCEMENT COOPERATION

The EDPB plays a key role in enforcing data protection laws. It ensures consistent enforcement and promotes enforcement cooperation amongst SAs. In addition, for a small number of complex cases on which SAs cannot agree via consensus, the EDPB takes binding decisions.

> *"Consistent enforcement is at the heart of the EDPB's work."*
>
> - Dr Andrea Jelinek, Chair of the EDPB

Since the General Data Protection Regulation (GDPR) started applying, the EDPB has focused attention and effort on ensuring consistent enforcement based on cooperation. Following the vision laid down in its 2021-2023 Strategy, this continues to be a high priority for the EDPB. In that respect, in 2022, the EDPB's work on enforcement cooperation shifted into a higher gear, particularly through the numerous initiatives taken to streamline enforcement cooperation among SAs.

It is worth highlighting the following initiatives:

- A number of taskforces have worked on key topics with a cross-border dimension. This has led to a consistent approach by the SAs on topics such as Google Analytics and cookie banners.
- Following the creation of the Coordinated Enforcement Framework in 2021 for simultaneous and coordinated enforcement actions by SAs, in 2022, 22 SAs undertook coordinated investigations into over 90 cloud services used in the public sector throughout the EEA.
- To support and increase SAs' capacity to supervise, investigate and enforce, the EDPB launched a Support Pool of Experts with

specialists in various areas, including IT auditing, security and data science.

All these efforts contribute to better internal work processes, unified strategies, enhanced cooperation and overall streamlining of the enforcement.

3.1.1. VIENNA STATEMENT ON ENFORCEMENT COOPERATION

In pursuit of developing a comprehensive and collaborative approach to address issues related to GDPR enforcement, the EDPB Members met in Vienna in April 2022 and reiterated their commitment to close cross-border cooperation. A statement summarised the Members' agreed action towards strong and swift enforcement of the GDPR through further enhancing cooperation on strategic cases and diversifying the range of cooperation methods used. Among other topics, the EDPB agreed to identify a list of procedural aspects that could be further harmonised in EU law to maximise the positive impact of GDPR cooperation. This list was sent to the European Commission for its consideration in October 2022, and was added to the European Commission's work programme for 2023.

Going forward, the EDPB will also prioritise enforcement actions by fostering greater cooperation on cross-border cases of strategic importance, addressing legal challenges stemming from matters of general application, and better aligning national enforcement strategies.

The EDPB Members are cognisant of the fact that this will represent a collaborative approach, with dedicated effort and cooperation from every member in improving the GDPR enforcement. As a consequence, this will result in greater robustness of the enforcement process and in ensuring a consistent interpretation of the GDPR.

Adopted: 28 April 2022

3.1.2. GUIDELINES 02/2022 ON THE APPLICATION OF ART. 60 GDPR

In line with the broader narrative to support effective enforcement and efficient cooperation between national SAs, the EDPB adopted Guidelines 02/2022 focusing on the interactions of SAs with each other, the EDPB and third parties under Art. 60 GDPR. The aim is to provide guidance in terms of cooperation and the One-Stop-Shop (OSS) mechanism. In practice, this helps SAs to enact their own national procedures in a manner consistent with the cooperation under the OSS mechanism.

The guidelines elaborate and clarify the requirements of each paragraph of Art. 60 GDPR, based on the provision's text and its practical implementation.

In terms of Art. 60(1) GDPR, the guidelines emphasise that the principles to be followed throughout the whole cooperation procedure are mutual obligations and that the SAs should endeavour to reach a consensual decision that is embedded in a process of mutual, consistent and timely exchange of all relevant information.

The guidance on Art. 60(2) GDPR focuses on the cooperative aspects in cases where the Lead Supervisory Authority (LSA) asks Concerned Supervisory Authorities (CSAs) to provide mutual assistance (Art. 61 GDPR) and conduct joint operations (Art. 62 GDPR).

The part dedicated to Art. 60(3) GDPR highlights the importance of collaborative interaction and early exchange of information between the LSA and the CSAs. More specifically, the guidelines clarify that the CSA should be able to contribute to the overall cooperation procedure and express their views even before the creation of a draft decision. In addition, the LSA is under the obligation to submit a draft decision in all cases of cross-border processing. The guidance on Art. 60(4)-(6) GDPR covers the potential scenarios that

follow the submission of a draft decision by the LSA and adds consistency to the post-submission procedure. The guidance on Art. 60(7)-(9) GDPR clarifies the distinction between notifying and informing SAs following the adoption of a binding decision.

To ensure further compliance after a final decision has been made by the LSA, the EDPB provides guidance on Art. 60(10) GDPR in terms of the obligations of the controller or processor in further processing activities in all its establishments.

Overall, the provided clarification and guidance of the requirements under Art. 60 GDPR significantly contribute to the desired consistency of the SAs' work and in enhancing enforcement cooperation.

Adopted: 14 March 2022

3.1.3. GUIDELINES 04/2022 ON THE CALCULATION OF ADMINISTRATIVE FINES UNDER THE GDPR

To harmonise the approach used by SAs in calculating fines, the EDPB adopted the first version of Guidelines 04/2022. The guidelines contribute to an important part of the EDPB's strategy in creating more efficient cooperation among SAs on cross-border cases.

> *"From now on, SAs across the EEA will follow the same methodology to calculate fines. This will boost further harmonisation and transparency of the fining practice of SAs. The individual circumstances of a case must always be a determining factor and SAs have an important role in ensuring that each fine is effective, proportionate and dissuasive."*
>
> - Dr Andrea Jelinek, Chair of the EDPB

The EDPB devised a systematic and chronological five-step methodology that SAs across the European Economic Area (EEA) can use for calculating administrative fines for infringements of the GDPR.

1. The SAs have to assess whether the case at stake concerns one or more sanctionable conducts and whether this has led to one or multiple infringements. Furthermore, in case one conduct gives rise to multiple infringements, it needs to be determined whether one infringement precludes the attribution of another infringement, or whether they are to be attributed alongside each other. The aim is to clarify which infringements can result in fines.
2. The SAs should use a harmonised starting point for the calculation of a fine, with three elements to consider: the categorisation of infringements by nature, the seriousness of the infringement and the turnover of the undertaking. This starting point forms the foundation for further calculations, and each assessment needs to be based on the merits of the case.
3. The SAs should also determine whether there are aggravating and mitigating circumstances (as listed in Art. 83 (2) GDPR) and increase or decrease the fine accordingly.
4. The SAs must ensure that fines do not exceed the legal maximums as set out in Art. 83(4)-(6) GDPR.
5. The SAs need to assess whether the calculated final amount meets the requirements of effectiveness, dissuasiveness and proportionality, or whether further adjustments to the amount are necessary.

The EDPB will regularly revise the guidelines and proposed methodology.

Adopted: 12 May 2022

3.2. 2022 ARTICLE 65 DECISIONS

The EDPB is empowered to issue binding decisions under Art. 65 GDPR to guarantee the consistent application of the GDPR by SAs. In 2022, the EDPB issued 5 binding decisions addressing a range of issues from right to access, right to object direct marketing, protection of children's use of social media to legal basis for processing personal data.

3.2.1. DECISION 01/2022 ON THE DISPUTE ARISEN ON THE DRAFT DECISION OF THE FRENCH SUPERVISORY AUTHORITY REGARDING ACCOR SA UNDER ART. 65(1)(A) GDPR

In June 2022, the EDPB settled a dispute regarding a fine against the French hospitality company Accor SA in its Decision 01/2022.

The French LSA issued a draft decision against Accor SA following complaints relating to a failure to consider the right to object to the receipt of marketing messages by mail and/or difficulties encountered in exercising the right of access. Upon sharing the draft decision with the CSAs, the Polish SA raised three objections, with a primary focus on the amount of the fine, which in its opinion was not effective, proportionate and dissuasive enough. The SAs did not reach a consensus on that given issue, henceforth it was referred to the EDPB pursuant to Art. 65(1)(a) GDPR.

The EDPB agreed with the reasoning of the Polish SA in certain aspects and decided that the French LSA needed to reassess the elements it relied upon to calculate the amount of the fine in order to ensure that it meets the criterion of dissuasiveness. The EDPB clarified that the fine should be determined solely based on the company's turnover of the preceding year, namely 2021, without considering the reduced turnover caused by the COVID-19 pandemic as a mitigating factor under 83(2)(k) GDPR.

The GDPR fine issued to Accor was increased from the initial EUR 100,000 imposed by the French LSA to EUR 500,000 following the EDPB's binding decision.

Adopted: 15 June 2022

3.2.2. BINDING DECISION 2/2022 ON THE DISPUTE ARISEN ON THE DRAFT DECISION OF THE IRISH SUPERVISORY AUTHORITY REGARDING META PLATFORMS IRELAND LIMITED (INSTAGRAM) UNDER ART. 65(1)(A) GDPR

In July 2022, the EDPB adopted a binding decision regarding Instagram, a unit of Meta Platforms Ireland Limited (Meta IE), particularly on the policy of maintaining public-by-default profiles of children and the mandatory public disclosure of their contact details when operating business accounts.

The Irish LSA triggered the dispute resolution procedure under Art. 65 GDPR after no compromise had been reached on the objections raised by several CSAs concerning the legal basis for processing and the determination of the fine.

In terms of publicly disclosing children's contact details when they operate business accounts, Meta IE relied on two legal bases for processing personal data: "performance of a contract" and "legitimate interests". The EDPB found that Meta IE could not have relied on Art. 6(1)(b) GDPR (performance of a contract) as a legal basis for the publication since the processing at stake was not necessary for the performance of a contract between Meta IE and its child users. Regarding the alternative legal basis of Art. 6(1)(f) GDPR (legitimate interests), the EDPB concluded that the publication of the children´s contact details did not meet the requirements because the processing was either unnecessary or, if it were to be considered necessary, it did not pass the balancing test required when determining legitimate interests.

Therefore, the EDPB concluded that Meta IE unlawfully processed children's personal data and it further instructed the Irish LSA to amend its draft decision by including the infringement of Art. 6(1) GDPR.

The EDPB also instructed the Irish SA to assess its envisaged administrative fine in accordance with Art. 83(1)-(2) GDPR to:

- Impose an effective, proportionate and dissuasive administrative fine for the additional infringement; and
- Ensure that the final amounts of the administrative fines are effective, proportionate and dissuasive.

On the issue of public-by-default profiles of children, initially raised as an objection by the Norwegian SA, the Irish SA was not required to amend its draft decision. Indeed, the EDPB concluded that the objection did not meet the requirements of being "relevant and reasoned" under Art. 4(24) GDPR since it was neither relevant nor sufficiently reasoned against the backdrop of the legal and factual content of the Irish SA's draft decision.

Following the EDPB's binding decision, the Irish LSA adopted its final decision against Meta IE. They determined that Meta IE had infringed Art. 6(1) GDPR. The final fine was the maximum of the EUR 202-405 million range which was initially envisaged in the draft decision.

> *"This is a historic decision. Not just because of the height of the fine - this is the second highest fine since the entry into application of the GDPR - it is also the first EU-wide decision on children's data protection rights. With this binding decision, the EDPB makes it extra clear that companies targeting children have to be extra careful. Children merit specific protection with regard to their personal data."*
>
> - Dr Andrea Jelinek, Chair of the EDPB

This EDPB decision has practical repercussions on the way this online platform operates its services in the EU. Meanwhile, Instagram has changed its practices. Accounts of people under 18 years of age are now private-by-default in the UK and EU, and the disclosure of contact details for business accounts is no longer mandatory.

Adopted: 28 July 2022

3.2.3. BINDING DECISION 3/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS FACEBOOK SERVICE (ART. 65 GDPR) AND BINDING DECISION 4/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS INSTAGRAM SERVICE (ART. 65 GDPR)

Following the EDPB's binding dispute resolution decisions of 5 December 2022, the Irish SA adopted its decisions regarding Facebook and Instagram (Meta IE). These decisions are the result of complaint-based inquiries into Facebook's and Instagram's activities in particular concerning the lawfulness and transparency of processing for behavioural advertising.

The binding decisions were adopted on the basis of Art. 65(1)(a) GDPR, after the Irish SA as LSA had triggered two dispute resolution procedures concerning the objections raised by concerned supervisory authorities (CSAs) from ten countries in each case. Among others, CSAs issued objections concerning the legal basis for processing (Art. 6 GDPR), data protection principles (Art. 5 GDPR), and the use of corrective measures including fines.

The EDPB decided that Meta IE inappropriately relied on contract as a legal basis to process personal data in the context of Facebook's Terms of Service and Instagram's Terms of Use for the purpose of behavioural advertising as this was not a core element of the services. The EDPB found in both cases that Meta IE lacked a legal basis for this processing and therefore unlawfully processed these data. As a consequence, the EDPB instructed the Irish SA to amend the finding in its draft decisions and to include an infringement of Art. 6(1) GDPR.

The EDPB instructed the Irish SA to include, in its final decisions, an order for Meta IE to bring its processing of personal data for behavioural advertising in the context of the Facebook and Instagram services into compliance with Art. 6(1) GDPR within three months.

Next, the EDPB examined whether the complaints had been addressed with due diligence. The complainant had raised the fact that sensitive data is processed by Meta IE. However, the Irish SA did not assess processing of sensitive data and therefore, the EDPB did not have sufficient factual evidence to enable it to make findings on any possible infringement of the controller's obligations under Art. 9 GDPR. As a result, the EDPB disagreed with the Irish SA's proposed conclusion that Meta IE is not legally obliged to rely on consent to carry out the processing activities involved in the delivery of its Facebook and Instagram services, as this could not be categorically concluded without further investigations. Therefore, the EDPB decided that the Irish SA must carry out a new investigation.

In addition, the EDPB instructed the Irish SA to include in both final decisions a finding of infringement of the principle of fairness and to adopt the appropriate corrective measures. The EDPB noted that the grave breaches of transparency obligations impacted the reasonable expectations of the users, that Meta IE had presented its services to users in a misleading manner, and that the relationship between Meta IE and users was imbalanced.

With respect to the administrative fines, the EDPB directed the Irish SA to impose an administrative fine for the additional infringements of Art. 6(1) GDPR (lack of legal basis for the processing of personal data) and to issue significantly higher fines for the transparency infringements identified, as it found the fines proposed did not fulfil the requirement of being effective, proportionate and dissuasive. This led to the Irish SA significantly increasing the fines in its final decisions (from a maximum of EUR 36 million and EUR 23 million for the Facebook and Instagram draft decisions, to EUR 210 million and EUR 180 million in the final decisions respectively).

3.2.4. BINDING DECISION 5/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA REGARDING WHATSAPP IRELAND LIMITED (ART. 65 GDPR)

Following the EDPB's binding dispute resolution decision of December 5th, WhatsApp Ireland Limited (WhatsApp IE) was issued a EUR 5.5 million fine by the Irish SA.

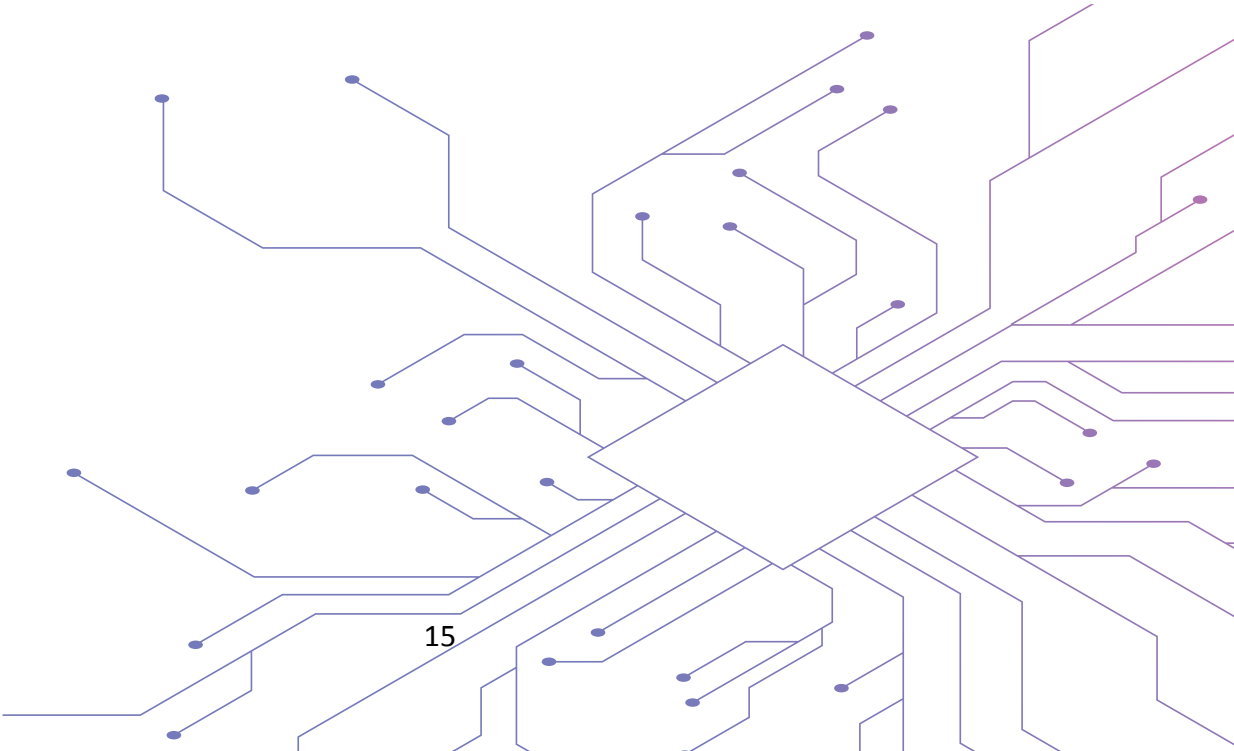
In its Binding Decision, the EDPB instructed the Irish SA to amend its draft decision with respect to the findings concerning lawfulness of the processing and the principle of fairness, and to the corrective measures envisaged.

Regarding the lawfulness of processing for Service improvement purposes, the EDPB decided that WhatsApp IE inappropriately relied on contract as a legal basis to process personal data. As a consequence, the EDPB instructed the Irish SA to add an infringement of Art. 6(1) GDPR. Additionally, the EDPB instructed the Irish SA to include an infringement of the principle of fairness under Art. 5(1)(a) GDPR.

The EDPB further decided that the Irish SA must carry out an investigation into WhatsApp IE's processing operations in order to determine whether it processes special categories of personal data (Art. 9 GDPR);

whether it processes data for the purposes of behavioural advertising, for marketing purposes, as well as for the provision of metrics to third parties and the exchange of data with affiliated companies for the purposes of service improvements.

With respect to corrective measures, the EDPB requested the Irish SA to include in its final decision an order for WhatsApp IE to bring its processing of personal data for the purposes of service improvement in the context of its Terms of Service into compliance with Art. 6(1) GDPR within a specified period of time, and to cover the infringements of Art. 6(1) GDPR with an administrative fine.



4

2022 - THE EDPB SECRETARIAT

4.1. THE EDPB SECRETARIAT

The EDPB Secretariat, which is provided by the European Data Protection Supervisor (EDPS), offers analytical, administrative and logistical support to the EDPB. The EDPB Secretariat is in charge of drafting EDPB documents, providing IT solutions to ensure transparent communications between all the European national Supervisory Authorities (SAs), handling EDPB media relations, as well as organising all EDPB meetings.

A Memorandum of Understanding establishes the terms of this cooperation between the EDPB and the EDPS. The staff at the EDPB Secretariat are employed by the EDPS, however, they work exclusively under the instructions of the Chair of the EDPB. At the end of 2022, the staff of the EDPB Secretariat was composed of 30 FTE staff members: one head of the EDPB Secretariat, 1 deputy head of unit, 1 head of sector, 4 heads of activity, 11 legal officers, 4 communication officers, 6 administrative assistants and 2 IT officers.

The EDPB Secretariat led the drafting of 26 opinions, binding decisions and statements adopted by the EDPB in 2022 and contributed to further 23 guidelines, opinions, binding decisions, statements and recommendations.

In 2022, the EPDB Secretariat organised 347 meetings for the EDPB, including 15 plenary meetings, 160 expert subgroup or taskforce meetings and 172 drafting teams. One significant distinction from previous years is that in 2022, the EDPB convened hybrid meetings for the first time. Out of 347 meetings, 34 were hybrid, whereas 308 were held remotely and 5 took place in-person.

4.2. EDPB BUDGET

The EDPB budget forms part of the broader budget of the EDPS. The financial resources provided to the data protection institutions allow them to fulfil their tasks, contribute to the implementation of the democratic values of the EU and the fundamental rights of privacy and data protection.

The EDPB budget for 2022 amounts to EUR 6,812,000 and covers all aspects related to the functioning of the EDPB. This includes, but is not limited to, expenditure for EDPB meetings at the plenary and subgroup level, translation and interpretation costs, IT services, and remuneration of the EDPB Secretariat staff.

4.3. IT COMMUNICATION TOOLS

In the context of cooperation between SAs, the EDPB Secretariat provides continuous support to SAs with IT solutions that facilitate their communication. In this respect, the EDPB Secretariat leads the IT Users Expert Subgroup, which focuses on the need for development and making changes to the information systems used by EDPB, including the Internal Market Information (IMI) system which is used to exchange information necessary for the GDPR cooperation and consistency mechanism. This included the overhaul of two procedures to reflect the experience gathered in the first years of the GDPR and updates to reflect modifications in the EDPB's Rules of Procedure. In addition, further reporting possibilities were introduced.

Throughout 2022, the EDPB Secretariat continued working on best practices to refine the procedures in use and to share its expertise on the use of the IMI system. While employing the IMI system, the SAs and the European Commission are supported by the EDPB IMI helpdesk within the EDPB Secretariat. The IMI helpdesk continued to carry out 3252 proactive monitoring procedures to ensure that case files were complete and registered correctly.

The EDPB Secretariat also performed a follow-up to the migration of the EDPB Wiki platform used for internal sharing of information, with additional functionalities and an enhanced user experience. In addition, the EDPB Secretariat upgraded the content management system (CMS) of the EDPB website 'https://edpb.europa.eu', which manages the creation and modification of digital content, to Drupal 9. A new advanced search feature to improve the usability of the website was introduced. The EDPB website was visited 275,734 times in 2022 and the most clicked topics are international transfer of data, General Data Protection Regulation, Data Protection Impact Assessment (DPIA) and code of conduct. Considerable efforts were made regarding the translation of documents available on the website. In fact, 283 EDPB documents and 159 press releases were translated into 22 languages.

The EDPB Secretariat improved internal tools for the organisation and planning of meetings and for the management of documents.

4.4. THE EDPB SECRETARIAT'S ACTIVITIES RELATING TO ACCESS TO DOCUMENTS

Transparency is a core principle of the EDPB. As an EU body, the EDPB is subject to Art. 15 of the Treaty of the Functioning of the European Union and Regulation 1049/2001 on public access to documents. Art. 76(2) GDPR and Art. 32 of the EDPB's Rules of Procedure reinforce this requirement. The principle of transparency provides any EU citizen, and any natural or legal person residing or having a registered office in a Member State, with the right of access to EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities. In exceptional cases, the EDPB may refuse to disclose all or part of a document. The reasons for such a refusal and corresponding procedural rules are outlined in Regulation 1049/2001 on public access to documents. In 2022, the EDPB

received 68 public access requests for documents held by the EDPB. Confirmatory applications were received in 7 cases[1]. In accordance with Art. 32(2) of the EDPB Rules of Procedure, the EDPB Secretariat prepares the answers to those requests, which are handled and signed by the Chair of the EDPB (for confirmatory applications) or one of the Deputy Chairs of the EDPB (for initial applications).

Three complaints regarding three EDPB's confirmatory decisions for requests for access to documents, submitted in 2021 and 2022, were brought to the attention of the European Ombudsman in 2022. Whilst the scope of the three complaints varied, their subject matter related to the US Foreign Account Tax Compliance Act (FATCA) and covered draft and final versions of statements, guidelines and letters, as well as correspondence. Following a reassessment of the requested documents, the EDPB decided to grant wider partial access to three documents, which were provided to the complainants. However, the EDPB informed the Ombudsman that access to most documents, mainly drafts, could not be granted in scope of these complaints, as several exceptions of Regulation 1049/2001 applied. Disclosure would have undermined the protection of privacy and the integrity of the individual (Art. 4(1)(b)) as well as the protection of the decision-making process at the EDPB (Art. 4(3)(2)). In particular, the EDPB argued that disclosing the draft documents would seriously jeopardize the EDPB's decision-making process, since the views of the EDPB members conveyed in the documents were at the time unknown to the public. The EDPB maintained that keeping the drafts from the general public is required for legal certainty, to avoid any confusion for stakeholders, as well as to ensure the consistent interpretation of EU data protection rules across the EU, and safeguard the EDPB's authority, independence and "space to think".

4.5. THE EDPB SECRETARIAT'S DATA PROTECTION OFFICER ACTIVITIES

The EDPB processes personal data following Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (Regulation 2018/1725). In accordance with Art. 43 of Regulation 2018/1725, the EDPB designated its own DPO team, which is part of the EDPB Secretariat, to handle the processing of personal data. The DPO's position and tasks are defined in Arts. 44 and 45 of Regulation 2018/1725, and are further detailed in the EDPB DPO Implementing Rules.

In 2022, the EDPB, with the assistance of its DPO team, continued to strengthen compliance with Regulation 2018/1725 by enhancing its transparency practices through different means, such as:

- development, publication and update of several privacy notices;
- continued development of several records, as well as publication of a centralised register for records on the EDPB website; and
- addition of new and updated information to its DPO website page.

The DPO team launched internal legal assessments on different issues concerning the EDPB's processing of personal data and identified suitable legal, organisational and, where applicable, technical solutions. The assessments were carried out as part of the DPO's advising function for the EDPB.

[1] According to Arts. 7 and 8 of the Regulation 1049/2001, when an application for access to documents is fully or partially refused, the applicant can file a confirmatory application, asking the institution to reconsider its position, within 15 working days (or as an exception, in 30 working days when the application relates to a long document or a large number of documents).

In 2022, the DPO team assisted with the handling of 6 data subject requests made on the basis of rights laid out in Art. 17 to Art. 24 of Regulation 2018/1725, which is the same figure as in 2021. The DPO team also provided assistance with replying to individual requests for information involving the processing of their personal data. In addition, the DPO team provided support in handling 12 data breaches under Arts. 34 and 35 of Regulation 2018/1725. The assessment of these data breaches revealed that a large majority of them was unlikely to pose a risk to the rights and freedoms of natural persons. Two data breaches required a notification to the EDPS.

Additionally, the DPO team delivered various internal training sessions and updated awareness-raising material aimed at EDPB Secretariat staff. These activities were tailored to the needs and expertise of the participants to ensure that all staff members were adequately informed of their responsibilities surrounding personal data processing, but also of their rights as data subjects.

Finally, the EDPB DPO team continued to maintain close relations with other EU institutions, bodies and agencies and their DPOs, particularly in matters involving or related to the processing of personal data. Such cooperation ensures the exchange of good practices, common experiences and tailored approaches to specific data protection challenges. To this end, the DPO team participated in the EU institutions' network of DPOs and the EDPB network of DPOs, comprising the DPOs of national SAs, the EDPS and the EDPB.

5 EUROPEAN DATA PROTECTION BOARD - ACTIVITIES IN 2022

5.1. BINDING DECISIONS

5.1.1. DECISION 01/2022 ON THE DRAFT DECISION OF THE FRENCH SUPERVISORY AUTHORITY REGARDING ACCOR SA UNDER ART. 65(1)(A) GDPR

See Section 3.2.1. for the full summary.

In June 2022, the EDPB resolved a dispute over a fine levied against the French hospitality company Accor SA. Initially, the French Lead Supervisory Authority (LSA) issued a draft decision against Accor SA, following the submission of complaints relating to difficulties when exercising the right to object to the receipt of marketing messages by email, and when exercising the right of access. The Polish SA voiced its objection to the decision as it considered the amount of the fine not to be sufficiently effective, proportionate and dissuasive.

Following the SAs' failure to reach consensus, the case was referred to the EDPB pursuant to Art. 65(1) GDPR. The EDPB agreed with the Polish SA's reasoning in certain aspects. Among others, it decided that the French LSA needed to reassess the elements it relied upon to calculate the amount of the fine in order to ensure that it meets the criterion of dissuasiveness.

Following the binding decision of the EDPB, the French SA imposed a fine of EUR 500,000 for infringements relating to the GDPR. In addition, the French SA imposed a fine of EUR 100,000 for infringements of the national transposition of the ePrivacy directive.

Adopted: 15 June 2022

5.1.2. BINDING DECISION 2/2022 ON THE DRAFT DECISION OF THE IRISH SUPERVISORY AUTHORITY REGARDING META PLATFORMS IRELAND LIMITED (INSTAGRAM) UNDER ART. 65(1)(A) GDPR

See Section 3.2.2. for the full summary.

In July 2022, the EDPB resolved a dispute regarding the Irish SA's draft decision on Instagram, a service of Meta Platforms Ireland Limited (Meta IE). Several SAs voiced their objection to the decision, and following the failure to reach consensus, the case was referred to the EDPB pursuant to Art. 65(1) GDPR.

In terms of publicly disclosing children's emails and/or phone numbers when they operate Instagram business accounts, the EDPB held that Meta IE could not rely on Art. 6(1)(b) GDPR (performance of a contract) or Art. 6(1)(f) GDPR (legitimate interests) and concluded that Meta IE infringed Art. 6(1) GDPR by processing children's personal data in an unlawful manner. The EDPB further requested the Irish SA to reassess its determination of the administrative fine in this case.

Following the EDPB's decision, the Irish SA issued a EUR 405 million fine to Meta IE, which at the time of writing was the second highest fine issued by an SA since the adoption of the GDPR.

Adopted: 28 July 2022

5.1.3. BINDING DECISION 3/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS FACEBOOK SERVICE (ART. 65 GDPR) AND BINDING DECISION 4/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS INSTAGRAM SERVICE (ART. 65 GDPR)

See Section 3.2.3. for the full summary.

The EDPB adopted the binding dispute resolution decisions on 5 December 2022, after the Irish SA as LSA had triggered two dispute resolution procedures concerning the objections raised by several Concerned Supervisory Authorities (CSAs) about the processing activities carried out by Meta IE in the context of the Facebook and Instagram services.

In its decisions, the EDPB affirmed that Meta IE inappropriately relied on contract as a legal basis to process personal data in the context of Facebook's Terms of Service and Instagram's Terms of Use for the purpose of behavioural advertising. Thereby, the EDPB found that Meta IE lacked a legal basis for this processing and instructed the Irish SA to order Meta IE to bring its processing into compliance with Art. 6(1) GDPR.

In addition, EDPB noted that the grave breaches of transparency obligations impacted the reasonable expectations of the users, that Meta IE had presented its services to users in a misleading manner, and that the relationship between Meta IE and users of Facebook and Instagram services was imbalanced.

The EDPB directed the Irish SA to impose an administrative fine for the additional infringements of Art. 6(1) GDPR (lack of legal basis for the processing of personal data) and to issue significantly higher fines for the transparency infringements. Following the decisions, Meta IE was issued hefty fines by the Irish SA.

Adopted: 5 December 2022

5.1.4. BINDING DECISION 5/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA REGARDING WHATSAPP IRELAND LIMITED (ART. 65 GDPR)

See Section 3.2.4. for the full summary.

In December 2022, the EDPB adopted a binding decision that requested the Irish SA to amend its draft decision regarding WhatsApp Ireland Limited (WhatsApp IE) with respect to the findings concerning the lawfulness of the processing and the principle of fairness, and to the corrective measures envisaged.

According to the EDPB, WhatsApp IE inappropriately relied on contract as a legal basis to lawfully process personal data for Service improvement purposes. The Irish SA was thereby instructed to add an infringement of Art. 6(1) GDPR, as well as to include an infringement of the principle of fairness under Art. 5(1)(a) GDPR.

Furthermore, the EDPB requested that the Irish SA carries out an investigation into WhatsApp IE's processing operations in order to determine whether it processes special categories of personal data (Art. 9 GDPR); whether it processes data for the purposes of behavioural advertising, for marketing purposes, as well as for the provision of metrics to third parties and the exchange of data with affiliated companies for the purposes of service improvements.

Following the binding dispute resolution decision, the Irish SA issued a EUR 5.5 million fine to WhatsApp IE.

Adopted: 5 December 2022

5.2. CONSISTENCY OPINIONS

5.2.1. OPINIONS ON DRAFT DECISIONS REGARDING BINDING CORPORATE RULES

SAs may approve Binding Corporate Rules (BCRs) within the meaning of Art. 47 GDPR.

BCRs are data protection policies implemented and adhered to within a group of enterprises established in the EEA for transfers of personal data outside the EEA within the same group. In 2022, several SAs submitted their draft decisions regarding the controller or processor BCRs of various companies to the EDPB, requesting an Opinion under Art. 64(1)(f) GDPR. The EDPB issued twenty-three opinions on BCRs.

In all instances, the EDPB concluded that the draft BCRs contained all required elements and guaranteed appropriate safeguards to ensure that the level of protection provided by the GDPR would not be undermined when personal data was transferred to and processed by the group members based in third countries. It is without prejudice to the obligation of the data exporter to assess whether, in the specific case, additional measures are necessary to ensure an essentially equivalent level of protection to that in the EU. In every case, based on the EDPB Opinions, the BCRs could be approved without changes by the relevant SAs.

The various opinions are listed below:

- Opinion 02/2022 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the WEBHELP Group Adopted: 7 February 2022;

- Opinion 03/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the WEBHELP Group Adopted: 7 February 2022;
- Opinion 04/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Norican Group Adopted: 18 March 2022;
- Opinion 05/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Lundbeck Group Adopted: 19 April 2022;
- Opinion 06/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Groupon International Limited Adopted: 19 April 2022;
- Opinion 07/2022 on the draft decision of the Hungarian Supervisory Authority regarding the Controller Binding Corporate Rules of MOL Group Adopted: 19 April 2022;
- Opinion 08/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Bioclinica Group Adopted: 4 May 2022;
- Opinion 09/2022 on the draft decision of the Danish Supervisory Authority regarding the Processor Binding Corporate Rules of Bioclinica Group Adopted: 4 May 2022;
- Opinion 10/2022 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Controller Binding Corporate Rules of Fresenius Group Adopted: 16 June 2022;
- Opinion 17/2022 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the ANTOLIN Group Adopted: 1 August 2022;
- Opinion 18/2022 on the draft decision of the Baden-Württemberg (Germany) Supervisory Authority regarding the Controller Binding Corporate Rules of the Daimler Truck Group Adopted: 26 August 2022;
- Opinion 19/2022 on the draft decision of the Baden-Württemberg (Germany) Supervisory Authority regarding the Controller Binding Corporate Rules of the Mercedes- Benz Group Adopted: 26 August 2022;
- Opinion 20/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ellucian Group Adopted: 26 August 2022;
- Opinion 21/2022 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Ellucian Group Adopted: 26 August 2022;
- Opinion 22/2022 on the draft decision of the Liechtenstein Supervisory Authority regarding the Controller Binding Corporate Rules of Hilti Group Adopted: 7 September 2022;
- Opinion 23/2022 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of the Samres Group Adopted: 7 September 2022;
- Opinion 24/2022 on the draft decision of the Swedish Supervisory Authority regarding the Processor Binding Corporate Rules of the Samres Group Adopted: 7 September 2022;
- Opinion 26/2022 on the draft decision of the Data Protection Authority of Bavaria for the Private Sector regarding the Controller Binding Corporate Rules of the Munich Re Reinsurance Group Adopted: 30 September 2022;

- Opinion 27/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of LEYTON Group Adopted: 7 October 2022;
- Opinion 29/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the DSV Group Adopted: 18 November 2022;
- Opinion 30/2022 on the draft decision of the Slovak Supervisory Authority regarding the Controller Binding Corporate Rules of the Piano Group Adopted: 28 November 2022;
- Opinion 31/2022 on the draft decision of the Slovak Supervisory Authority regarding the Processor Binding Corporate Rules of the Piano Group Adopted: 28 November 2022;
- Opinion 32/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ramboll Group Adopted: 06 December 2022.

5.2.2. OPINIONS ON DRAFT REQUIREMENTS FOR ACCREDITATION OF A CERTIFICATION BODY

Three SAs submitted their draft decisions on accreditation requirements for certification bodies under Art. 43(1)(b) GDPR to the EDPB, requesting an opinion under Art. 64(1)(c) GDPR. These requirements allow the accreditation of certification bodies responsible for issuing and renewing certification in accordance with Art. 42 GDPR.

These opinions aim to establish a consistent and harmonised approach regarding the requirements that SAs and national accreditation bodies apply when accrediting certification bodies under the GDPR. To do so, the EDPB made recommendations to the relevant SAs on the amendments to be made to the draft accreditation requirements. The SAs then amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various opinions are listed below:

- Opinion 11/2022 on the draft decision of the competent Supervisory Authority of Poland regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 4 July 2022;
- Opinion 12/2022 on the draft decision of the competent Supervisory Authority of France regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 4 July 2022;
- Opinion 13/2022 on the draft decision of the competent Supervisory Authority of Bulgaria regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 4 July 2022.

5.2.3. OPINIONS ON CERTIFICATION CRITERIA

When an SA intends to approve a certification pursuant to Art. 42(5) GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR through the consistency mechanism referred to in Arts. 63, 64 and 65 GDPR. Under this framework, according to Art. 64(1)(c) GDPR, the EDPB is required to issue an opinion on an SA's draft decision approving the certification criteria. The EDPB issued three opinions on certification criteria in 2022, aiming at ensuring the consistent application of the GDPR, including by the SAs, controllers and processors.

The three opinions are listed below:

- Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria Adopted: 8 February 2022;

- Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors Adopted: 22 September 2022;
- Opinion 28/2022 on the Europrivacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR) Adopted: 10 October 2022.

5.2.4. OPINIONS ON SAS' APPROVAL OF ACCREDITATION REQUIREMENTS FOR CODE OF CONDUCT MONITORING BODY

The EDPB issued three opinions on draft accreditation requirements for code of conduct monitoring bodies, as requested by SAs in accordance with Art. 64(1)(c) GDPR.

The aim of these EDPB opinions is to ensure consistency and the correct application of the requirements among SAs. To do so, the EDPB made several recommendations to the various SAs on the amendments to be made to the draft accreditation requirements. On this basis, the SAs amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various opinions are listed below:

- Opinion 14/2022 on the draft decision of the competent Supervisory Authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR Adopted: 4 July 2022;
- Opinion 15/2022 on the draft decision of the competent Supervisory Authority of Luxembourg regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR Adopted: 4 July 2022;
- Opinion 16/2022 on the draft decision of the competent Supervisory Authority of Slovenia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 4 July 2022.

5.3. GENERAL GUIDANCE

5.3.1. GUIDELINES 01/2022 ON DATA SUBJECT RIGHTS - RIGHT OF ACCESS

The guidelines provide further clarity on the right of access, a cornerstone right of data subjects that is enshrined in Art. 8 of the EU Charter of Fundamental Rights. It has been a part of the European data protection framework since its beginning and has been further developed by more precise rules in Art. 15 GDPR.

With the exceptions referred to in the GDPR and analysed in the guidelines, the right of access allows data subjects to obtain full disclosure of their personal data. Unless explicitly stated otherwise, the request should be understood as referring to all personal data concerning the data subject. The right of access includes three different components:

i. confirmation as to whether data about the person is processed or not;
ii. access to this personal data; and
iii. access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers.

The guidelines provide clarifications on the scope of the right of access, the information the controller has to provide to the data subject, the format of the access request, the main modalities for providing access and the limits and restrictions of the right. The controller

may ask the data subject to specify the request if they process a large amount of data. Even data that may be incorrect or unlawfully processed will have to be provided. At the same time, the guidelines elaborate on the limits and restrictions of the right. The guidelines provide examples to support controllers in answering access requests in a GDPR-compliant manner.

Adopted: 18 January 2022

5.3.2. GUIDELINES 02/2022 ON THE APPLICATION OF ART. 60 GDPR

See Section 3.1.2. for the full summary.

The EDPB adopted Guidelines 02/2022 with the aim of providing guidance on cooperation between SAs and on the One-Stop-Shop (OSS) mechanism. In practice, the guidelines help SAs to enact their own national procedures in a manner consistent with the cooperation under the OSS mechanism. The guidelines elaborate and clarify the requirements of each paragraph of Art. 60 GDPR, based on the provision's text and its practical implementation. Overall, the provided guidance significantly contributes to the desired consistency of the SAs' work and to enhancing enforcement cooperation.

Adopted: 14 March 2022

5.3.3. GUIDELINES 03/2022 ON DECEPTIVE DESIGN PATTERNS IN SOCIAL MEDIA PLATFORM INTERFACES: HOW TO RECOGNISE AND AVOID THEM

The EDPB Guidelines 03/2022 aim to help designers and users of social media platforms in deciding how to assess and avoid deceptive design (so-called "dark patterns") that infringe on GDPR requirements. The Guidelines define dark patterns as "interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data".

The categories of dark patterns addressed in the Guidelines are: a) overloading, b) skipping, c) stirring, d) hindering, e) fickle and f) left in the dark.

These Guidelines provide examples of deceptive design in use cases of the life cycle of a social media account (i.e. from the sign-up stage to the closing of a social media account).

In addition to the examples of deceptive design, the Guidelines include best practices at the end of each use case (i.e. specific recommendations for designing user interfaces that facilitate the effective implementation of the GDPR).

Adopted: 14 March 2022

5.3.4. GUIDELINES 04/2022 ON THE CALCULATION OF ADMINISTRATIVE FINES UNDER THE GDPR

See Section 3.1.3. for the full summary.

The guidelines contribute to an important part of the EDPB's strategy based on creating more efficient cooperation among SAs on cross-border cases, by harmonising the approach used by SAs in calculating fines. The EDPB devised a systematic and chronological five-step methodology that SAs across the European Economic Area (EEA) can use for calculating administrative fines for infringements of the GDPR. The circumstances of the specific case are the determining factors leading to the final amount, which can – in all cases – vary between any minimum amount and the legal maximum.

Adopted: 12 May 2022

5.3.5. GUIDELINES 05/2022 ON THE USE OF FACIAL RECOGNITION TECHNOLOGY IN THE AREA OF LAW ENFORCEMENT

Increasingly, law enforcement authorities (LEAs) are showing an interest in the use of facial recognition technology (FRT). This technology often relies on artificial intelligence (AI) or machine learning (ML) and can be used, for example, to search for persons on police watch lists or to monitor the movements of an individual in public space.

FRT relies on the processing of biometric data, which benefit from special protection in the legal framework. Indeed, biometric data are permanently and irrevocably linked to an individual's identity, and therefore carry significant data protection implications.

Through its guidelines, the EDPB outlines the applicable legal framework that lawmakers at the national and EU level, as well as LEAs using the FRT systems, must strictly comply with to ensure data subjects' rights.

The guidelines also provide a tool to support a first classification of a given use case (Annex I) as well as practical guidance for LEAs that plan to procure and run an FRT-system. Further, the guidelines include a set of hypothetical situations illustrating concrete uses of FRT and relevant considerations, especially regarding the necessity and proportionality test.

Adopted: 12 May 2022

5.3.6. GUIDELINES 06/2022 ON THE PRACTICAL IMPLEMENTATION OF AMICABLE SETTLEMENTS

Through these guidelines, the EDPB discusses the power to reach an amicable settlement as well as the role of the amicable settlement in the context of the One-Stop-Shop mechanism. It analyses the legal consequences and includes practical recommendations, proposing a step-by-step guide for handling a case via amicable settlement.

In the context of complaint handling by SAs, most Member States see amicable settlements as a process of "alternative dispute resolution". In most cases, the amicable settlement solution is relied on where a complaint is lodged with the SA concerning an alleged violation of the GDPR, in particular concerning data subjects' rights, to resolve the case in the data subjects' favour. In such cases, the settlement is to be reached between the controller and the data subject, under the supervision of the SA, which moderates the course of events.

The EDPB recognises that amicable settlements are tools to achieve compliance with the GDPR by the controller. In case a complaint is lodged because a controller has not fulfilled the data subject rights pursuant to Art. 12 to Art. 22 GDPR, the enforcement of data subject rights can be expedited by an amicable arrangement between the actors.

Adopted: 18 November 2021; formatting changes made on 12 May 2022

5.3.7. GUIDELINES 07/2022 ON CERTIFICATION AS TOOL FOR TRANSFERS

In its Art. 46, the GDPR requires data exporters to put in place appropriate safeguards for transfers of personal data to third countries or international organisations. To that end, the GDPR distinguishes appropriate safeguards that may be used by data exporters under Art. 46 for framing transfers to third countries by introducing, amongst others, certification as a new transfer mechanism (Arts. 42(2) and 46(2)(f) GDPR).

These guidelines provide guidance on the application of Art. 46(2)(f) GDPR regarding transfers of personal data to third countries or to international organisations on the basis of certification.

First, the EDPB underlines that the nature of these guidelines is complementary to the general Guidelines 1/2018 on certification. The guidelines specify the requirements for transfers under GDPR when certification is used. In this respect, the EDPB clarifies the obligations of the data exporter and the data importer, with a special focus on the latter, who will be granted the certification.

In addition, the EDPB provides guidance on the certification criteria already listed in Guidelines 01/2018 and establishes additional specific criteria that should be included in a certification mechanism used as a tool for transfers to third countries, such as the assessment of the third country legislation, the rules on onward transfers and redress and enforcement. Lastly, the guidelines discuss the elements that should be addressed in the binding and enforceable commitments that controllers or processors not subject to the GDPR should take in order to provide appropriate safeguards for data transferred to third countries.

Adopted: 14 June 2022

5.3.8. GUIDELINES 8/2022 ON IDENTIFYING A CONTROLLER OR PROCESSOR'S LSA

These guidelines constitute a targeted update of the Article 29 Working Party's guidelines for identifying a controller or processor's LSA (paragraphs 29-34 and points I and III under 2.d. of the Annex), previously endorsed by EDPB. The document gives further clarifications on the notion of main establishment in the context of joint controllership and builds on the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

Adopted: 10 October 2022

5.3.9. GUIDELINES 9/2022 ON PERSONAL DATA BREACH NOTIFICATION UNDER GDPR

The Article 29 Working Party guidelines on personal data breach notification under Regulation 2016/679 guidelines, previously endorsed by the EDPB, outline the mandatory breach notification and communications requirements of the GDPR and provide suggestions for how controllers and processors can fulfil these obligations. In the targeted update of these guidelines, the EDPB clarifies the notification requirements concerning personal data breaches at non-EU establishments. The updated guidelines specify that data controllers who are not established in the EU will need to notify data breaches to every single authority for which affected data subjects reside in their Member State. The mere presence of a representative in a Member State does not trigger the one-stop-shop system.

Adopted: 10 October 2022

5.3.10. GUIDELINES ADOPTED AFTER PUBLIC CONSULTATION

5.3.10.1. GUIDELINES 01/2021 ON EXAMPLES REGARDING PERSONAL DATA BREACH NOTIFICATION

The EDPB adopted these practice-oriented and case-based guidelines to help data controllers in deciding how to handle personal data breaches and what factors to consider during risk assessment.

The guidelines address six categories of personal data breaches and outline several examples of typical situations based on the SAs' experience. The categories of personal data breaches addressed in the guidelines are as follows:

1. **Ransomware attacks** which involve malicious code encrypting personal data, where the attacker requests a ransom in exchange for a decryption code.
2. **Data exfiltration attacks** which exploit vulnerabilities in services offered over the internet and usually aim to copy, exfiltrate and abuse personal data for some malicious end.
3. **Internal human-related risk source** which refers to human errors leading to personal data breaches, which can have a frequent occurrence and can be both deliberate or accidental, therefore making it difficult for data controllers to identify weaknesses and take steps to avoid them.
4. **Loss or theft of devices and/or documents** which is a frequent occurrence of a data breach that might present a difficult risk assessment when devices are no longer available.
5. **Mispostal** which involves internal human error in setting the recipient(s) of a communication. The error occurs due to inattentiveness without any malicious intention.
6. **Social engineering** which refers to psychological manipulation attacks involving identity theft and email exfiltration.

For each category of personal data breaches the guidelines provide advisable, but not exclusive or comprehensive, practical measures to be considered both when dealing with data breaches and for future prevention.

Adopted: 14 January 2021 and adopted in its final version following public consultation on 14 December 2021

5.3.10.2. GUIDELINES 04/2021 ON CODES OF CONDUCT AS TOOLS FOR TRANSFERS

In accordance with Art. 46 GDPR, controllers and processors shall put in place appropriate safeguards for transfers of personal data to third countries or international organisations. Therefore, the GDPR distinguishes the appropriate safeguards that may be used by organisations under Art. 46 for framing transfers to third countries by introducing, amongst others, codes of conduct as a new transfer mechanism (Arts. 40(3) and 46(2)(e) GDPR). Controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards.

In the guidelines, the EDPB underlines that, in terms of content, such codes should address the essential principles, rights and obligations arising under the GDPR for controllers and processors and include guarantees that are specific to the context of transfers, such as onward transfers or conflict of laws in the third country. Striving towards a practical implementation of the guidelines, the EDPB provides a checklist of the elements to be covered.

These guidelines, which complement the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, provide clarification as to the role of the different actors involved for the setting of a code to be used as a tool for transfers and the adoption process displayed through flow charts.

Adopted: 7 July 2021; formatting changes made on 22 February 2022

5.4. REGISTER FOR DECISIONS TAKEN BY SA AND COURTS ON ISSUES HANDLED IN THE CONSISTENCY MECHANISM

The EDPB maintains a publicly accessible electronic register of decisions taken by SAs and courts on issues handled in the consistency mechanism per Art. 70(1)(y) GDPR. This register provides for accessibility and transparency of the decisions and further promotes the consistent application of the GDPR by the European SAs.

All decisions added in 2022 are related to decisions made by the SAs following the EDPB consistency opinions or following the 01/2022 EDPB binding decision on the dispute arisen on the draft decision of the French SA regarding Accor SA.

See Section 5.2 on consistency opinions and Section 5.1 on binding decisions.

5.5. LEGISLATIVE CONSULTATION AND DOCUMENTS ADDRESSED TO THE EU INSTITUTIONS OR NATIONAL AUTHORITIES

5.5.1. EDPS-EDPB JOINT OPINION 1/2022 ON THE EXTENSION OF THE COVID-19 CERTIFICATE REGULATION

On 3 February 2022, the European Commission adopted, firstly, a Proposal for a Regulation on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic for EU citizens, and secondly, a Proposal for a Regulation on the same matters, but applying to third-country nationals legally staying or residing in the territories of Member States.

As a general remark, the EDPB and the EDPS recall in their opinion that compliance with data protection rules does not constitute an obstacle to fighting the COVID-19 pandemic and that, at the same time, the general principles of effectiveness, necessity and proportionality must guide any measure adopted by Member States or EU institutions that involve the processing of personal data to fight COVID-19. In addition, the EDPB and the EDPS underline that any restriction to the free movement of persons within the European Union put in place to limit the spread of SARS-CoV-2, including the requirement to present EU Digital COVID Certificates, should be lifted as soon as the epidemiological situation allows.

The EDPS and EDPB take note that the European Commission did not carry out an impact assessment for the Proposals, due to the urgency and their limited scope. They strongly consider that the Proposals should be accompanied by an impact assessment report, in order to provide a clear justification on the necessity and proportionality, taking into account the evolution of the epidemiological situation with regard to the COVID-19 pandemic together with the impact on fundamental rights and non-discrimination.

Lastly, the EDPB and the EDPS invite the Commission to assist the Member States in developing technical specifications on the recognition of information about the COVID-19 vaccine and the number of doses administered to the holder, regardless of the Member State in which they have been administered.

Adopted: 14 March 2022

5.5.2. EDPB-EDPS JOINT OPINION 2/2022 ON THE PROPOSAL OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HARMONISED RULES ON FAIR ACCESS TO AND USE OF DATA (DATA ACT)

In a joint effort, the EDPB and the EDPS comment on overarching concerns related to the Proposal for the Data Act and urge the co-legislator to take decisive action. While welcoming the efforts made to ensure that the Proposal does not affect the current data protection framework, the EDPB and the EDPS consider that additional safeguards are necessary to avoid lowering the protection of the fundamental rights to privacy and to the protection of personal data in practice. Their comments concern three distinct areas: i) the rights to access, use and share data, ii) the obligation to make data available in case of "exceptional need", and iii) the implementation and enforcement.

First, the Joint Opinion stresses the need for provisions explicitly specifying that data protection law "prevails" in case of conflict with the provisions of the Proposal insofar as the processing of personal data is concerned. In addition, a more robust application of the data minimisation principle is encouraged when designing new products. Along with that, the Opinion calls for an enhancement of the right to data portability. In general, the EDPB and the EDPS stress the need to ensure that access, use, and sharing of personal data by users other than data subjects, as well as by third parties and data holders, should occur in full compliance with all of the provisions of the GDPR, EUDPR and ePrivacy Directive.

Second, the EDPB and the EDPS express concerns regarding the lawfulness, necessity and proportionality of the obligation to make data available to public sector bodies and EU institutions, agencies or bodies in case of "exceptional need". They remind that any limitation of the right to protection of personal data must be based on a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand its scope.

Third, regarding implementation and enforcement, the EDPB and the EDPS highlight the risk of operational difficulties that might result from the designation of more than one competent authority responsible for the application and enforcement of the Proposal. At the same time, they welcome the designation of the data protection SAs as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned, and they ask the co-legislators to also designate national SAs as coordinating competent authorities under this Proposal.

Adopted: 4 May 2022

5.5.3. EDPB-EDPS JOINT OPINION 03/2022 ON THE PROPOSAL FOR A REGULATION ON THE EUROPEAN HEALTH DATA SPACE

The EDPB and the EDPS jointly expressed their views on the proposed Regulation on the European Health Data Space. The resulting opinion first notes that the Proposal aims at: i) supporting individuals to take control of their own health data, ii) supporting the use of health data for better healthcare delivery, better research, innovation and policy making, and iii) enabling the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data. However, they are concerned that the Proposal may weaken the protection of the rights to privacy and to data protection, especially considering the categories of personal data and purposes that are related to the secondary use of data. They also note that the Proposal will add yet another layer to the already complex (multi-layered) collection of provisions (to be found both in the EU and Member States law) on the processing of health data (in the health care sector).

In that respect, the EDPB and the EDPS consider that it is important to clarify the relationship between the provisions in the Proposal with the ones in the GDPR and Member State laws. Additionally, with regards to the scope, they recommend excluding wellness applications and other digital applications, as well as wellness and behaviour data relevant to health. Should this be maintained, the EDPB and the EDPS suggest that personal data deriving from wellness apps and other digital health applications should not be included in the secondary use of health data, as they do not have the same data quality requirements and characteristics as those generated by medical devices. Further, they strongly recommend not extending the scope of the GDPR exceptions regarding the data subject's rights and note the need to remain consistent with the relevant GDPR provisions.

The EDPB and the EDPS are of the view that the Proposal should further delineate purposes for secondary use and circumscribe when there is a sufficient connection with public health and/or social security.

Lastly, the EDPB and the EDPS acknowledge that the infrastructure for the exchange of electronic health data foreseen in the Proposal will not establish a central EU-database of health data and will only facilitate the exchange of such health data from decentralised databases. However, due to the large quantity of data that would be processed and their highly sensitive nature, among others, the EDPB and the EDPS call for a requirement for storing the personal electronic health data in the EU/EEA, without prejudice to further transfers in compliance with Chapter V of the GDPR.

Adopted: 12 July 2022

5.5.4. EDPB-EDPS JOINT OPINION 04/2022 ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN RULES TO PREVENT AND COMBAT CHILD SEXUAL ABUSE

In relation to the European Commission's Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, the EDPB and the EDPS adopted a joint opinion on 28 July 2022. While emphasizing the gravity of child sexual abuse as a serious and heinous crime, the Opinion expresses serious concerns regarding the proportionality of the envisaged interference and limitations to the protection of the fundamental rights to privacy and the protection of personal data.

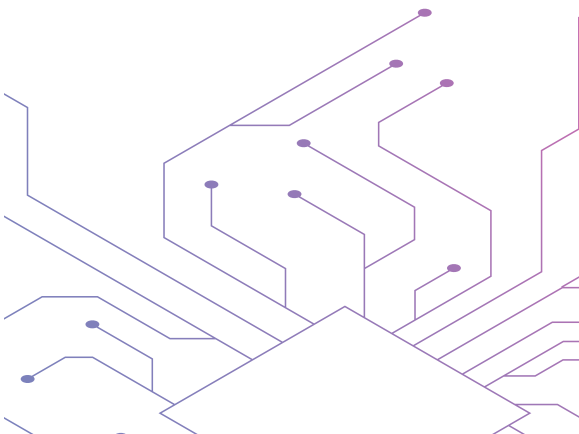
The EDPB and EDPS note that the Proposal's lack of detail, clarity, and precision regarding the conditions for issuing a detection order for child sexual abuse material (CSAM) and child solicitation does not ensure that only targeted approaches to detecting CSAM are used. They raise the concern that the Proposal could potentially be used as a basis for generalised and indiscriminate scanning of the content of all types of electronic communications. As a result, the EDPB and EDPS recommend that the conditions for issuing detection orders be further clarified to address these concerns.

Additionally, the EDPB and EDPS raise concerns about the measures envisaged for the detection of unknown CSAM and the solicitation of children in interpersonal communication services, in particular due to likelihood of errors and their high level of intrusiveness into the privacy of individuals. Overall, the EDPB and the EDPS argue that the requirement imposed on online service providers to decrypt online communications in order to block those related to CSAM is disproportionate to the aim pursued.

The EDPB and EDPS underline that breaking or weakening encryption in order to access private communications would have a substantial impact on the right to private life and to the confidentiality of communications, freedom of expression, innovation and growth of the digital economy.

Lastly, the EDPB and EDPS recommend that the relationship between the tasks of the national Coordinating Authorities under the Proposal and SAs be better regulated. They also underline that the transmission of personal data between the newly proposed EU Centre and Europol should only take place following a duly assessed request case-by-case.

Adopted: 28 July 2022



5.5.5. STATEMENT 01/2022 ON THE ANNOUNCEMENT OF AN AGREEMENT IN PRINCIPLE ON A NEW TRANS-ATLANTIC DATA PRIVACY FRAMEWORK

The GDPR requires that the European Commission seeks an opinion of the EDPB before adopting a possible new adequacy decision recognising as satisfactory the level of data protection guaranteed by a third country. In principle, the EDPB welcomes the announcement of a political agreement between the European Commission and the United States on 25 March 2022 on a new Trans-Atlantic Data Privacy Framework. This announcement is made at a time when transfers from the EEA to the U.S. face significant challenges.

The EDPB looks forward to carefully assessing the improvements that a new Trans-Atlantic Data Privacy Framework may bring in light of the EU law, the case law of the CJEU and the recommendations EDPB made on that basis. In particular, the EDPB will analyse in detail how these reforms ensure that the collection of personal data for national security purposes is limited to what is strictly necessary and proportionate.

Lastly, the EDPB will examine to what extent the announced independent redress mechanism respects the EEA individuals' right to an effective remedy and to a fair trial. In particular, the EDPB will look at whether any new authority involved in this mechanism has access to relevant information, including personal data, when exercising its mission and can adopt decisions binding on the intelligence services, and whether there is a judicial remedy against this authority's decisions or inaction.

Adopted: 6 April 2022

5.5.6. STATEMENT 04/2022 ON THE DESIGN CHOICES FOR A DIGITAL EURO FROM THE PRIVACY AND DATA PROTECTION PERSPECTIVE

In its Statement, the EDPB emphasises the importance of ensuring a very high standard of privacy and data protection by design and by default in the digital euro project. To meet this standard, the EDPB suggests that different design choices should be considered and adopted based on a documented impact assessment prioritising innovative and privacy-enhancing technologies.

The EDPB cautions against the use of systematic validation and tracing of all transactions in digital euro. In this regard, the EDPB advises that the digital euro be made available both online and offline, along a threshold below which no tracing is possible, in order to guarantee full anonymity of daily transactions.

The EDPB also welcomes the European Commission's intention to propose in 2023 a specific legal framework for the digital euro, for which it stands ready to provide relevant guidance. Finally, the EDPB urges the European Central Bank and the European Commission to enhance public debate on the digital euro project to ensure it meets the highest standards of privacy and data protection.

Adopted: 10 October 2022

5.5.7. RESPONSE OF THE EDPB TO THE EUROPEAN COMMISSION'S TARGETED CONSULTATION ON A DIGITAL EURO

In April 2022, the European Commission launched a public consultation to gather information on the expected impact of the digital euro on stakeholders, including with regard to its privacy and data protection aspects.

In its contribution to this consultation, the EDPB recalls the views it expressed to the European institutions in a letter of June 2021, namely that a high level of data protection and privacy rights is crucial to strengthen end-users' trust in the digital euro project, and thus to ensure its acceptance by European citizens. In order to achieve this, the EDPB recommends that the features of the digital euro be designed as closely as possible to physical cash.

In particular, the EDPB stresses the importance of providing individuals with a bearer-based architecture available both online and offline. Furthermore, the EDPB is of the opinion that controls of transactions should only be carried out by the competent authorities and reduced to the minimum necessary. Finally, the EDPB recommends that such transactions should not be traceable at all below a certain threshold.

Adopted: 14 June 2022

5.5.8. STATEMENT ON THE IMPLICATIONS OF THE CJEU JUDGMENT C-817/19 ON THE USE OF PNR IN MEMBER STATES

Following the CJEU judgment on the Directive (EU) 2016/681 (also referred to as the "PNR Directive") on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, the EDPB adopted a Statement on 13 December 2022.

In its ruling, the CJEU set out strict limitations which must be observed by a Member State when transposing and applying the PNR Directive. The limitations that stand out as the most relevant ones are:

- limitation to the purposes set out in the PNR Directive, which are exhaustive;
- application of the PNR system only to terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air and thus also exclusion of ordinary crime;
- limitation of the application of the PNR Directive with regard to intra-EU flights and other means of transport; and
- no indiscriminate application of the general retention period of five years to all air passengers' personal data.

In response to the judgment, the EDPB, through its Statement, asked Member States to take all necessary steps to guarantee that their national implementations of the PNR Directive are in line with the fundamental right to the protection of personal data, as laid down in Art. 8 of the EU Charter of Fundamental Rights. Steps taken by the Member States must include legislative measures as well as the identification of measures that can be adopted promptly in practice.

Adopted: 13 December 2022

5.6. OTHER GUIDANCE AND INFORMATION NOTES

5.6.1. STATEMENT 02/2022 ON PERSONAL DATA TRANSFERS TO THE RUSSIAN FEDERATION

Recent geopolitical developments had Russia excluded from the Council of Europe on 16 March 2022. Although Russia continues to be a contracting party to conventions and protocols concluded in the framework of the Council of Europe to which it has expressed its consent to be bound, for instance, Convention 108, the modalities of Russia's participation in these instruments are still to be determined.

In its Statement, the EDPB recalls that the transfer of personal data to a third country, in the absence of

an adequacy decision of the European Commission pursuant to Art. 45 GDPR, is only possible if the controller or processor has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies are available for data subjects (Art. 46 GDPR), or in specific circumstances, only on one of the conditions set forth in Art. 49 GDPR.

Russia does not benefit from an adequacy finding by the European Commission in accordance with Art. 45 GDPR. Therefore, the EDPB notes that, when personal data are transferred to Russia, data exporters under the GDPR should assess and identify the legal basis for the transfer and the instrument to be used among those provided by Chapter V GDPR (e.g., Standard Contractual Clauses or Binding Corporate Rules), in order to ensure the application of appropriate safeguards.

SAs of EEA Member States which have close economic and historic ties with Russia are already looking into the lawfulness of data transfers to Russia, including in the context of ongoing investigations. They will handle cases involving data transfers to Russia, taking into account the increased impact on the rights and freedoms of data subjects that may arise from such data processing operations, and will coordinate within the EDPB, as appropriate.

Adopted: 12 July 2022

5.7. GDPR COOPERATION AND ENFORCEMENT

5.7.1. STATEMENT ON ENFORCEMENT COOPERATION

On 28 April 2022, the EDPB adopted a Statement on enforcement cooperation, following a high-level meeting in Vienna where EDPB members agreed to enhance cooperation on strategic cases and to diversify the range of cooperation methods used.

The Statement recalls the SAs' commitment to close cross-border cooperation. The SAs agree to collectively and regularly identify cross-border cases of strategic importance, with the EDPB's support, in different Member States. Additionally, SAs commit to further exchanging information on national enforcement strategies in order to reach an agreement on annual enforcement priorities at the EDPB level.

The Statement also reiterates the EDPB's role in ensuring a consistent interpretation of the GDPR. The EDPB shall deal with specific legal issues on matters of general application as well as facilitate the cross-border exchange of information. Lastly, in order to maximise the positive impact of GDPR cooperation, the EDPB set out to identify a list of procedural aspects that can be further harmonised in EU law.

For more on the Statement on enforcement cooperation see Section 3.1.1.

Adopted: 28 April 2022

5.7.2. EDPB DOCUMENT ON THE SELECTION OF CASES OF STRATEGIC IMPORTANCE

Following the Vienna meeting of April 2022, the EDPB adopted a document that establishes criteria for determining whether a case is of strategic importance, in line with the Statement on enforcement cooperation. The EDPB considers cases to be of strategic importance if there is a high risk to the rights and freedoms of natural persons in several Member States.

Pursuant to the document, a proposal voluntarily submitted by an SA may qualify as a case of strategic importance if it concerns a structural or recurring problem in several Member States, is related to the intersection of data protection with other legal fields, and/or affects a large number of data subjects in several Member States. Cases that involve a large

number of complaints in several Member States, a fundamental issue falling within the scope of the EDPB strategy, and/or matters where the GDPR implies that high risk can be assumed, also qualify as strategically important cases.

Further, the EDPB lays down in its document the process and timeline for the selection of cases. A template for the proposal of a strategic case is also provided by the EDPB, to ensure that Member States include all the information relevant to the case when submitting their proposal.

5.7.3. COORDINATED ENFORCEMENT FRAMEWORK

Ever since the implementation of the GDPR, the EDPB has emphasised the importance of consistent enforcement through cooperation efforts. Hence, in line with its 2021-2023 Strategy, the EDPB set up a Coordinated Enforcement Framework (CEF), which provides a structure for recurring annual coordinated action by SAs. The CEF works to facilitate joint actions in a coordinated and flexible manner, including activities such as joint awareness campaigns, information gathering, enforcement sweeps as well as joint investigations. Annual coordinated efforts are intended to improve compliance, empower individuals to exercise their rights and increase awareness of data protection issues.

In 2022, the EDPB considerably increased its efforts to streamline enforcement cooperation, particularly through various initiatives focused on improving cooperation among SAs. During the year, as a result of effective cooperation, EDPB members launched their first coordinated action on the use of Cloud-based services by the public sector.

For more on enforcement cooperation, see Section 3.1.

5.7.4. SUPPORT POOL OF EXPERTS

As part of its 2021-2023 Strategy, the EDPB established a Support Pool of Experts (SPE) in 2020. The SPE's main objective is to assist SAs in carrying out investigations and enforcement activities of significant common interest. The SPE provides support in the form of expertise for investigations and enforcement activities of common interest to SAs and enhances cooperation/solidarity by reinforcing and complementing the strengths of the individual SAs and addressing operational needs. This includes but is not limited to, analytical support, assistance in the performance findings of a forensic nature, as well as in the preparation of investigative reports on the basis of evidence collected. Further, the SPE enhances the cooperation and solidarity between all EDPB members by sharing, reinforcing and complementing strengths and addressing operational needs.

A call for external experts was launched and at the end of 2022, the SPE was composed of 409 external experts.

5.8. PLENARY MEETINGS AND SUBGROUPS

In the period between 1 January and 31 December 2022, the EDPB held 15 plenary meetings.

The agendas and minutes of these meetings are published on the EDPB website. The outcome of the plenary meetings consists of adopted guidelines, opinions and other documents such as statements or information notes to advise the European Commission, national SAs and other stakeholders on data protection matters, with a primary focus on the GDPR. Additionally, there were 160 expert subgroup meetings and 172 drafting team meetings. In total, 347 meetings were held, including plenary meetings, expert subgroup meetings, task force meetings and drafting team meetings.

The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks. Chapter 9 outlines the list of the expert subgroups and their respective mandates.

5.9. STAKEHOLDER CONSULTATION

5.9.1. STAKEHOLDER EVENTS

The EDPB invited various NGOs to the 69th Plenary meeting to discuss challenges caused by differences in national administrative law. Participants acknowledged the importance of the Vienna meeting and the EDPB statement on enforcement cooperation. They indicated that a significant number of the issues they faced with the One-Stop-Shop were caused by differences in national procedural law. The NGO representatives notably discussed the procedural issues faced when lodging complaints. Constructive criticism was given in the context of the SAs' duty to decide on a complaint, specifically regarding the lack of information they provide to the complainants.

The NGOs stressed that in order to ensure the right to a legal remedy, every complaint must lead to a formal decision. They further advocated for clear deadlines for each step of the cooperation procedure and identified issues related to the informal closing or narrowing down the scope of complaints. Additionally, the NGOs addressed, among others, the notification of decisions. Finally, the NGOs stated that reopening the GDPR at this stage was unnecessary.

5.9.2. PUBLIC CONSULTATION ON DRAFT GUIDANCE

Following the preliminary adoption of guidelines, the EDPB organises public consultations to give stakeholders and citizens the opportunity to provide additional input. The EDPB Members and the EDPB Secretariat in charge of drafting the guidelines consider this input before adopting the guidelines in their final version.

To increase transparency, the stakeholders' contributions to public consultations are published by the EDPB on its website. In 2022, the EDPB launched several consultations:

- In January, the EDPB opened public consultations on Guidelines 01/2022 on data subject rights - Right of access. There were 72 contributions made to the guidelines from a mix of entities such as business associations, NGOs, companies, research institutions and consumer organisations. Natural persons also contributed to the public consultation.
- In March, Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them were open for public consultations. A total of 26 contributions were made to these guidelines. Contributors were mostly DPO entities and NGOs.
- Later in May, the EDPB opened public consultations on both Guidelines 04/2022 on the calculation of administrative fines under the GDPR and Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Guidelines 04/2022 received feedback from 33 entities, whereas Guidelines 05/2022 received 14 contributions. While contributors to the former Guidelines are in majority DPO entities and business associations, Guidelines 05/2022 received feedback from a mix of contributors such as public authorities, academic institutions and NGOs.
- In late June, public consultations were opened for Guidelines 07/2022 on certification as a tool for transfers. A total of 20 contributions were made, nine of which were written by business associations.
- Two guidelines were also published for consultation in October, namely: Guidelines 8/2022 on identifying a controller or processor's

lead supervisory authority and Guidelines 9/2022 on personal data breach notification under GDPR. There were six contributions to Guidelines 8/2022, and 20 contributions to Guidelines 9/2022.

- Lastly, in November, the EDPB invited feedback on Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), which were accepting contributors until 10 January 2023. Regarding these recommendations, 15 contributions were submitted.

5.9.3. SURVEY ON PRACTICAL APPLICATION OF ADOPTED GUIDANCE

The EDPB conducted the fifth annual survey as part of its review of activities under Art. 71(2) GDPR. The survey focused on EDPB's work and output in 2022 – particularly its guidelines, joint opinions and consultation work – to determine the usefulness of its guidance for interpreting GDPR provisions and to identify ways to better support organisations and individuals in navigating the EU data protection framework.

The survey collected the opinions of various key stakeholders with diverse interests and concerns regarding EU data protection law, in order to gather a comprehensive insight into how the EDPB's work in 2022 was perceived in the data protection and privacy sector. Among the individuals surveyed were privacy and IT experts, representatives of EU DPO organisations, as well as academics and lawyers in the field of data protection and privacy rights. The questions asked were based on a standardised questionnaire. The collected data was synthesised and common themes were identified.

In general, the surveyed stakeholders agreed that the EDPB's guidelines and joint opinions were coherent, pertinent and provided examples of practical value. Specific praises were given to the Guidelines 9/2022 on personal data breach notification under GDPR, which stakeholders noted offered better examples compared to guidelines adopted in previous years. Indeed, examples were deemed clear and could be easily relied on to address real-life scenarios. With regard to Guidelines 06/2022 on the practical implementation of amicable settlements, a limited number of stakeholders argued that the examples, despite being generally good, sometimes lacked clarity.

The surveyed stakeholders confirmed that they consult EDPB guidelines and joint opinions on a near-daily basis for professional purposes. It was notably indicated that the stakeholders made use of the EDPB's guidance as a basis of interpretation when dealing with different applicable laws. Most stakeholders transform the EDPB's guidelines and recommendations into practical tools to implement high-level policies. However, they also noted the challenge of swiftly doing such a transformation due to the dissimilar structure of the guidelines.

Stakeholders also pointed out that the guidelines are easily readable for experts in the field of data protection, while acknowledging that the language used is somewhat too technical for the larger public and key concepts could be made more succinct. Suggestions were made to release shorter, supplementary versions of final documents, as well as consider the adoption of infographics and hashtags of key terms to render the data more accessible. Additionally, stakeholders expressed the urgency for faster implementation of new guidelines and their revisions after public consultation.

With respect to consultations and workshops organised by the EDPB, participants expressed a desire for a more transparent overview of how their

suggestions were incorporated into the documents after the consultation process.

Regarding the accessibility of EDPB guidance on its website, stakeholders are largely satisfied. Indeed, they noted a substantial enhancement in the communication and openness of the EDPB.

In terms of the EDPB's future work, stakeholders showed their support for guidelines on the role of DPOs, as well as for updated guidance on anonymisation and pseudonymisation. Stakeholders also expressed the need for the EDPB to take a stronger standpoint when dealing with adequacy-related issues. Some stakeholders also find that guidelines covering multiple topics are harder to read than documents focusing on sector-specific issues. Thereby, they underlined the importance of adopting more sectorial guidelines in the future.

Overall, the EDPB received high praise for the quality of the guidance it provided in 2022 and was especially recognised for its success in clarifying complex GDPR concepts through the production of comprehensive documents.

The EDPB greatly values the engagement and input from stakeholders in its work and strives to implement such input in its 2023 activities. The feedback on the value of the guidance and general work of the EDPB was appreciated as it provided useful insights into the needs of stakeholders. The EDPB intends to persist in maintaining and strengthening the coherence of its efforts in the future.

5.10. EXTERNAL REPRESENTATION OF THE BOARD

Public awareness and cooperation are vital to upholding data protection rights in the EEA and beyond, which is why the EDPB values stakeholder and citizen engagement. When the Chair and Deputy Chairs of the EDPB engage with other EU institutions or bodies, or when they, or the EDPB Staff represent the EDPB at conferences and multi-stakeholder platforms, they are supported by the EDPB Secretariat. Staff from the EDPB Secretariat themselves participate in several events to promote EDPB's activities. As such, the EDPB participates in various groups and summits, such as the Global Privacy Assembly, the G7 DPA roundtable,

ENISA Advisory Group, Stakeholder Cybersecurity Certification Group.

As Chair of the EDPB, Andrea Jelinek, had more than 26 speaking engagements in 2022. These speaking engagements included press briefings, presentations and panel discussions for a range of institutes, academic forums and policy agencies. During the year, the Chair also met with European Commissioners, as well as representatives from UNESCO and the Council of the EU Working Party on Information Exchange and Data Protection, among others. Furthermore, she attended several seminars and summits on data protection and privacy matters.

In 2022, Deputy Chairs Ventsislav Karadjov and Aleid Wolfsen took part in four speaking engagements which consisted of speeches, presentations and panel discussions at several conferences and forums.

A total of 38 events were attended both physically and virtually by the EDPB Staff. These events were largely hosted by, amongst others, universities, law firms, companies and EU institutions.

6

SUPERVISORY AUTHORITY ACTIVITIES IN 2022

6.1. CROSS-BORDER COOPERATION

Under the GDPR, national Supervisory Authorities (SAs) have a duty to cooperate to ensure the consistent application of data protection law. In cases that have a cross-border component, the SAs of the European Economic Area (EEA), i.e. the 27 EU Member States plus Iceland, Norway and Liechtenstein, have a range of tools at their disposal to facilitate harmonisation.

These tools are:

- Mutual assistance;
- Joint operations;
- The One-Stop-Shop (OSS) cooperation mechanism.

6.1.1. PRELIMINARY PROCEDURE TO IDENTIFY THE LEAD AND CONCERNED SUPERVISORY AUTHORITIES

Before starting an OSS procedure for a cross-border case, it is necessary to identify the Lead Supervisory Authority (LSA) and the other Concerned Supervisory Authorities (CSAs).

The LSA is identified as the SA of the EEA country where the data controller or processor under investigation has its main establishment. To identify a controller's or processor's main establishment, one key criterion is the place of central administration. Further information on this subject is available in the Article 29 Working Party Guidelines for identifying a controller's or processor's LSA, endorsed by the EDPB at its first plenary meeting on 25 May 2018.

The EDPB created workflows in the Internal Market Information System (IMI) to enable SAs to identify their respective roles. This IT platform is used to support cooperation and consistency procedures under the GDPR. The main purpose of this procedure is to define roles at an early stage.

In case of conflicting views regarding which SA should act as LSA, the EDPB acts as a dispute resolution body and issues a binding decision.

From 1 January 2022 to 31 December 2022, there were 624 instances in which LSAs and CSAs were identified.

6.1.2. DATABASE REGARDING CASES WITH A CROSS-BORDER COMPONENT

A case with a cross-border component is registered in a central database via the IMI and may occur in several situations:

- When the data controller or processor has an establishment in more than one Member State;
- When the data processing activity substantially affects individuals in more than one Member State; and/or
- When SAs are simply exchanging information, i.e. providing each other with mutual assistance.

Between 1 January and 31 December 2022, there were 310 entries in the database out of which 254 originated from a complaint, while 56 had other origins, such as investigations, legal obligations and/or media reports.

Please note that:

- References to case register entries in these statistics do not have a 1-to-1 correlation to the number of cross-border complaints handled per country as multiple complaints may be bundled in one case register entry, which therefore can relate to multiple cross-border cases;
- Depending on the Member State legislation, supervisory authorities may have handled complaints outside of the Art 60 procedure in accordance with their national law.

6.1.3. ONE-STOP-SHOP MECHANISM AND DECISIONS

The OSS mechanism demands cooperation between the LSA and the CSAs. The LSA leads the investigation and plays a key role in the process of reaching a consensus between the CSAs, in addition to working towards reaching a coordinated decision.

The LSA must first investigate the case while taking into account national procedural rules. During this phase, the LSA can gather information from another SA via mutual assistance or by conducting a joint investigation. The IMI also gives the LSA the opportunity to informally communicate with all CSAs to collect relevant information.

Once the LSA has completed its investigation, it prepares a draft decision, which it communicates to the CSAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, the EDPB acts as a dispute resolution body and issues a binding decision. The LSA must adopt its final decision on the basis of the EDPB's decision.

Between 1 January 2022 and 31 December 2022, there were 714 OSS procedures, which resulted in 330 final decisions.[2]

[2] Please note that this may include as well '*sui generis*' decision in the meaning of paragraph 38 of the EDPB Guidelines 06/2022 on the prac-

The IMI offers different procedures that can be followed when handling OSS cases:

- Informal consultation procedures;
- Draft decisions or revised decisions submitted by the LSA to the CSAs; and/or
- Final OSS decisions submitted to the CSAs and the EDPB.

The OSS case register is a valuable resource to showcase how SAs work together to enforce the GDPR. It offers an exceptional opportunity to read final decisions taken by, and involving, different SAs relating to specific data subject rights.

6.1.3.1. CASE DIGEST ON THE RIGHT TO OBJECT

This section offers a case digest which analyses decisions relating to Art. 17 (right to erasure) and 21 GDPR (right to object).[3] The case digest was commissioned as part of the EDPB's Support Pool of Experts initiative, which aims to support cooperation among SAs by providing expertise and tools related to enforcement.[4]

6.1.3.1.1. THE RIGHT TO OBJECT AND ITS RELATIONSHIP WITH THE RIGHT TO ERASURE IN DATA SUBJECT COMPLAINTS

The application of Art. 21 GDPR (right to object) is often combined with the exercise of the right to erasure, as enshrined in Art. 17 GDPR. Art. 17(1) GDPR recognises this right when the data subject objects to processing pursuant to Art. 21(1) GDPR and there are no overriding legitimate grounds for data processing,[5] or when the data subject objects to data processing performed for direct marketing purposes pursuant to Art. 21(2) GDPR.

Most of the cases decided by SAs under Art. 21 GDPR deal with the use of personal data for direct marketing (Art. 21(2) GDPR), rather than objections to the processing of data in the performance of tasks carried out in the public interest, in the exercise of official authority vested in the controller, or on the basis of legitimate interests (Art. 21(1) GDPR). **Thus, in the cases examined, there is a frequent link between the request to stop any further processing of personal data for marketing purposes[6] and the request to erase previously collected data.**

Against this background, two main sets of issues characterise the case law on Art. 21 GDPR, as emerging from the decisions adopted within the cooperation mechanism provided for in Art. 60 GDPR: (i) issues

tical implementation of amicable settlements.

[3] The analysis is based on the information gathered and the outcomes of the relevant inspection activities carried out as referred to by the SAs in their final decisions. This may entail some limitations in having a comprehensive view of individual cases.

Finally, since in the vast majority of cases the right to erasure is associated with right to object, the case law on Art. 21 GDPR is discussed before the decisions relating to Art. 17. This follows the most common sequence of requests that the SAs have to deal with and whose order contributes to shaping their decisions.

[4] This thematic section was produced by Alessandro Mantelero (9 December 2022), who was contracted in the framework of the Support Pool of Experts.

[5] See Section III.3 below.

[6] Art. 21(2) and Art. 21(3) GDPR.

concerning effective exercising of the right to object by data subjects, and (ii) issues relating to the procedure adopted by data controllers and processors in handling complaints from data subjects.

6.1.3.1.2. EXERCISE OF THE RIGHT TO OBJECT

Three particular elements relevant to the exercise of the right to object are highlighted: (i) the information provided to the data subject about the right to object,[7] (ii) the solutions – including technical solutions – adopted to make the exercise of this right easier, and (iii) the implementation of appropriate procedures to handle such requests. The first two elements are discussed in this section, while the last one is covered in Section 6.1.3.3.

Several cases concern non-compliance with the GDPR because the controller did not provide data subjects with any **information on the right to object**, in contrast with Art. 13(2)(b) GDPR [EDPBI:ES:OSS:D:2021:263].[8] One such case decided in 2021 concerned a complainant receiving direct marketing by email from a bank without receiving information about the right to object to the processing of personal data for direct marketing purposes, pursuant to Art. 21(4) GDPR [EDPBI:NO:OSS:D:2021:292]. Data subjects were targeted with direct marketing emails without having the option to opt out when registering their email addresses, and were only able to do so by changing their preferences once they had accessed the online banking service, or by contacting customer service.[9]

This case is also relevant in highlighting some recurring shortcomings in the **technical and organisational solutions** adopted by controllers in dealing with this type of request. These include lack of capacity and backlogs in customer service departments [EDPBI:NO:OSS:D:2021:292], as well as incorrect processing of objection requests [EDPBI:EE:OSS:D:2019:55], where the data subject's request was not properly registered resulting in the implementation of the objection with regard to only one account in a case of multiple user accounts and technical errors within the system [EDPBI:CZ.OSS:D:2021:312] creating delays in complying with Art. 21 GDPR.[10]

It is worth noting that the controller is required to facilitate the exercise of data subject rights[11] and that, in the context of information society services, the right to object may be exercised by automated means using technical solutions.[12] Although shortcomings regarding the exercise of the right to object are often part of a broader lack of compliance by data controllers, a focus on the design of the legal and technical solutions used to enable the exercising of this right plays a crucial role in terms of compliance.[13]

---

[7] See also, *inter alia*, CJEU, case C-201/14, *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*, para 33.

[8] See Recital 70 relating to the right to object for direct marketing.

[9] In this case, the LSA issued a reprimand and ordered the controller to implement measures to ensure that personal data is no longer processed for direct marketing when so requested by data subjects and to ensure that data subject requests under Art. 15 to Art. 22 GDPR are answered within the time limits set in Art. 12(3) GDPR.

[10] See also Art. 12(3) GDPR.

[11] See Article 29 Working Party guidelines on transparency under Regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, available at https://ec.europa.eu/newsroom/article29/items/622227/en, accessed 10.10.2022, 26-27. These guidelines were endorsed by the EDPB on 25 May 2018.

[12] See Art. 21(5) GDPR.

[13] See e.g. EDPBI:FR:OSS:D:2019:73; EDPBI:FR:OSS:D:2019:8.

Finally, as regards how this right can be exercised, in the cases reviewed the data subjects were not asked for a request in legal terms, as even a generic request not to receive further marketing messages (such as "I ask for a guarantee that this will not repeat itself", EDPBI:NO:OSS:D:2021:292) could be considered appropriate.

6.1.3.1.3. COMPLAINTS HANDLING PROCEDURE

Most of the cases decided under Art. 60 GDPR show deficiencies in the internal procedure adopted to deal with such requests,[14] including related aspects such as the accuracy of the procedure and internal communication,[15] the timeframe for processing requests,[16] and accountability (e.g. evidence that a system for receiving/tracking complaints has been put in place).[17]

Legal design elements play an important role in enabling the right to object in relation to this procedural dimension. **Cumbersome procedures** and **language barriers** should be avoided.[18] This should prevent cases such as the one when a contact email address was provided for the exercise of data subjects' rights, but an automated response referred the data subject to the "Contact us" form on the website, thus setting up a cumbersome procedure instead of directly handling the requests through the contact email [EDPBI:FR:OSS:D:2022:326].

The design of interaction with the data subject must therefore be carefully considered, using a clear and easily accessible form (see Art. 12 GDPR)[19] and avoiding any misunderstanding. For example, when using a no-reply email address for marketing purposes, data subjects must be informed in a clear manner and in the body of such emails that the message does not allow replies to the sender and, therefore, that any objections expressed by replying will be ineffective.[20] In addition, emails acknowledging receipt of objection requests must provide data subjects with timely information on the timeframe for implementation of their requests; data subjects must then be correctly informed about the outcome of the exercise of their rights.[21]

Specific procedures to process objection requests – including appropriate technical solutions – must therefore be adopted by data controllers, involving data processors according to the task distribution relating to processing operations,[22] being aware that

---

[14] See EDPBI:DEBE:OSS:D:2021:184; EDPBI:ES:OSS:D:2021:263; EDPBI:NO:OSS:D:2021:292; EDPBI:CZ.OSS:D:2021:312; EDPBI:-FR:OSS:D:2022:326.

[15] See EDPBI:UK:OSS:D:2019:31.

[16] See EDPBI:DEBE:OSS:D:2018:9.

[17] See EDPBI:CY:OSS:D:2019:57; EDPBI:CY:OSS:D:2019:58; EDPBI:FR:OSS:D:2020:84.

[18] See Art. 12 GDPR. See also Article 29 Working Party, Guidelines on transparency under Regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, available at https://ec.europa.eu/newsroom/article29/items/622227/en, accessed 10.10.2022, 10. These guidelines were endorsed by the EDPB on 25 May 2018.

[19] See Art. 12 GDPR. See also EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted - version for public consultation, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en, accessed 20.11.2022, 42-44.

[20] See e.g. EDPBI:FR:OSS:D:2019:8.

[21] See EDPBI:EE:OSS:D:2019:55 and EDPBI:FR:OSS:D:2019:41.

[22] See e.g. EDPBI:FR:OSS:D:2020:84, EDPBI:MT:OSS:D:2019:60, and EDPBI:EE:OSS:D:2019:55.

an incorrect task allocation may delay an appropriate response.[23]

In addition, the technical solutions implemented must be effective and **designed with the different types of data subject in mind.** For example, it is inappropriate to use an unsubscribe link at the bottom of direct marketing emails referring to a specific customer account page, since prospects who do not have a customer account cannot unsubscribe via this link. Here, a link that directly unsubscribes the user is much more effective than referring to the customer account.[24]

Although setting up specific procedures for exercising the right to object is desirable, it is worth noting that this should not limit data subjects' possibilities to send requests to the controller in other ways. However, **informal requests**, such as through a tweet on Twitter, can legitimately be disregarded by the controller when other more formal channels, such as email, are available [EDPBI:SE:OSS:D:2021:276]. Establishing specific and appropriate procedures that data subjects can use for their requests helps handle them carefully, whereas leaving room for the initiative may lead to difficulties, such as when data subjects' requests are sent using a different email address than the one used to create the personal account.[25]

Finally, to ensure effective regulatory compliance, **accountability** plays a crucial role in terms of record-keeping of the objection requests and their outcome.[26] A **data controller is responsible** for mistakes of its employees in dealing with data subjects' requests, and the employee's fault is irrelevant in assessing compliance with the GDPR and proving accountability in the cases examined [EDPBI:DEBE:OSS:D:2021:184].

6.1.3.2. CASE DIGEST OF THE RIGHT TO ERASURE

6.1.3.2.1. THE RIGHT TO ERASURE IN CASE LAW UNDER ART. 60 GDPR

Despite the significant development of the right to be forgotten in the online context after the Google Spain case,[27] very few decisions have been adopted over the years by SAs on this topic under Art. 60 GDPR.[28] The large majority of the cases deal with requests for: (i) erasure as a result of objecting to the processing of data for marketing purposes [e.g., EDPBI:CZ:OSS:D:2021:312],[29] including unsolicited emails [e.g., EDPBI:NO:OSS:D:2022:314], and (ii) erasure of accounts/profiles relating to services no longer used.[30]

As the cases examined largely concern fairly basic situations, at least from the point of view of compliance with Art. 17 GDPR, the main considerations are: (i) bottlenecks and shortcomings in the internal

[23] See EDPBI:UK:OSS:D:2019:31 in a case where the customer care officer had forwarded the data subject's request to the wrong department.

[24] See e.g. EDPBI:FR:OSS:D:2020:84.

[25] See also EDPBI:MT:OSS:D:2019:60 and Section III.2 on the right to erasure.

[26] See also EDPBI:CY:OSS:D:2019:57; EDPBI:CY:OSS:D:2019:58.

[27] CJEU, case C 131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, available at https://curia.europa.eu.

[28] This is probably due to the fact that many of them are handled as local cases under Art. 56(2) GDPR. See the Internal EDPB Document 1/2019 on handling cases with only local impacts under Art. 56(2) GDPR, Example 11, page 10.

[29] See also EDPBI:DEBE:OSS:D:2018:9 and Section II.1.

[30] See e.g. EDPBI:DESL:OSS:D:2019:11.

complaints handling procedure, and (ii) the presence of an overriding legitimate interest or other conditions justifying the processing despite the request for erasure. In view of the large number of requests they receive, data controllers usually put in place partially or fully automated procedures to deal with them.

As for the right to erasure, complaint procedures can be divided into two main steps: the exercise of the right based on the data subject's request (see para 6.1.3.2.2.) and the complaints handling procedure (see para 6.1.3.2.3.). As a result, the issues related to these two phases are different, focusing more on the correct identification of the data subject as far as erasure requests are concerned, and more on the classification of requests and internal organisation as regards the complaint handling phase.

6.1.3.2.2. EXERCISE OF THE RIGHT TO ERASURE

As in cases relating to the right to erasure, the data controller must **facilitate the exercise of the data subject's right**[31] without creating cumbersome procedures. In this regard, critical issues concern the identification of the data subject and the **proof of identification**.[32] Although Art. 12(6) GDPR allows the data controller to ask for additional information in event of reasonable doubt as to the identity of a data subject, a specific assessment is required to determine whether a reasonable doubt exists.[33]

Additional information for the purposes of Art. 12(6) GDPR should therefore be justified on a case-by-case basis. Requiring a copy of a national ID card by default is not acceptable.[34] The undue request of identity documents as a condition for the exercise of the right to erasure violates the principle of data minimisation pursuant to Art. 5(1)(c) GDPR. Failure to comply with such a request cannot therefore justify delaying the erasure of the data and, as the data subject's personal data could have been deleted at the time of the request, the continued processing of personal information after receipt of the erasure request constitutes an infringement of Art. 6(1) GDPR.[35]

A common argument used to justify the need to provide an official identity document relates to the problem raised by sending the erasure request via an **email address other than the one used at the registration stage**. Although in such cases the identity of the data subject may be uncertain on the basis of the sole email address, other solutions more in line with the minimisation principle are available. It would, for example, be disproportionate to require a copy of an identity document in the event where the data

---

[31] Art. 12(2) GDPR.

[32] See e.g. EDPBI:DK:OSS:D:2019:69.

[33] See also Recital 64 GDPR and Article 29 Working Party, Guidelines on the right to "data portability" (wp242rev.01), available at https://ec.europa.eu/newsroom/article29/items/611233/en, accessed 10.10.2022, 13, and EDPBI:FR:OSS:D:2019:3 (the online nature of the customer relationship cannot in itself imply such a reasonable doubt and be a sufficient reason to require a proof of identity; the latter must be justified by specific circumstances, such as suspicion of identity theft or account piracy). These guidelines were endorsed by the EDPB on 25 May 2018.

[34] See also EDPBI:FR:OSS:D:2019:3 (the practice of requiring individuals to "systematically provide a copy of an identity document for exercising their rights [...] does not, in view of its systematic nature, comply with the text [of the applicable law]") and EDPBI:IE:OSS:D:2020:166 (in a case where the standard procedure of the data controller was to ask for the submission of a copy of a national identity card for all erasure requests, the LSAs had made it clear that "the request for a copy of a national identity card was not made on foot of any specific doubt as to the complainant's identity, but rather was a result of the policy that was in place in Groupon at the time") and EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted - version for public consultation, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en, accessed 20.11.2022, 23-27.

[35] See EDPBI:IE:OSS:D:2020:166.

subject made their request within an area where they are already authenticated.[36] Conversely, it is possible, for example, to provide a unique identifier to users at the end of the registration process,[37] to inform users that only requests from an email address linked to their profile will be taken into account, to provide a password hotline in order to change the account login details,[38] to use other means of identification, such as via an online call,[39] or to identify the claimant by asking for additional information related to the service (e.g. current and previous nicknames, date of account registration, secret questions) [EDPBI:EE:OSS:D:2021:294].

In the case of robot-generated requests, the measures taken by data controllers to cope with the increased workload generated by these types of requests, cannot limit the exercise of the subject's rights by adopting **semi-automated procedures for sending erasure requests** that lead to disregarding any requests that do not follow the instructions.[40]

Furthermore, in the cases of Art. 17(1) GDPR, including ones in which the data subject withdraws consent (Art. 17(1)(b) GDPR) or objects to processing under Art. 17(1)(c) GDPR, a specific request of erasure from the data subject is not necessary, as there is an independent obligation arising for the data controller to delete data regardless of the request[41] [EDPBI:DEBE:OSS:D:2021:229].

6.1.3.2.3. THE COMPLAINTS HANDLING PROCEDURE

An effective exercise of the right to erasure requires adequate management of the internal processes. This is especially true when requests are on a large scale, as in the case of erasure based on objections to data processing for marketing purposes. In this context, different types of shortcomings may occur that jeopardise the effective exercise of the data subject's right.

The main shortcomings detected by the LSAs can be classified under two categories, namely **procedural shortcomings and human errors**, where the former are more impactful in terms of GDPR compliance as they affect all requests handled, while the latter are case specific.

Among the procedural shortcomings, the most serious concerned the **complete absence of a specific procedure to deal with erasure requests**,[42] while the most frequent case concerns delays in the erasure

---

[36] See EDPBI:FR:OSS:D:2019:3.

[37] See EDPBI:DK:OSS:D:2019:69.

[38] See also EDPBI:LU:OSS:D:2019:14 and EDPBI:LU:OSS:D:2020:94.

[39] See also EDPBI:MT:OSS:D:2019:26.

[40] See EDPBI:DK:OSS:D:2020:151.

[41] See EDPBI:DEBE:OSS:D:2021:229 as well as the EDPB Opinion 39/2021 on whether Art. 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject, paragraph 22 ("Article 17 GDPR provides for both (i) an independent right for data subjects and (ii) an independent obligation for the controller. In this regard, Article 17 GDPR does not require the data subject to take any specific action, it merely outlines that the data subject "has the right to obtain" erasure and the data controller "has the obligation to erase" if one of cases set forth in Article 17(1) GDPR applies") and paragraph 23 ("some cases set forth in Article 17(1) GDPR clearly refer to scenarios that the controllers must detect as part of their obligation for erasure, independently of whether or not the data subjects are aware of these cases").

[42] See also e.g. EDPBI:MT:OSS:D:2019:60.

process due to **poor internal organisation**[43] or technical malfunction, which is why, for example, the data controller must adopt appropriate technical solutions not to leave an old contact email address unmonitored (e.g., automatic reply informing about the new contact email address or an automatic re-directing to the correct email) [EDPBI:MT:OSS:D:2021:212].[44]

The relationship between data controller and data processor, if not properly managed, may also lead to **lack of coordination/instructions in the handling of requests**, with the result that the effective exercise of the right to erasure may be impaired.[45]

In some limited cases, **inadequate technological solutions** are the main reason for the failure to fully meet the data subject's requests, such as when documents sent by users via email to the data controller have been stored by generating URL links making their subsequent deletion more difficult [EDPBI:FR:OSS:D:2021:202, in a case where customers' driving licenses were accessible via any browser without required authentication by entering a URL that linked to the software used for data storage].[46]

Finally, in several cases, the data controller complied with the data subject's request for erasure but **did not inform the data subject** of the erasure (Art.l 12(3) GDPR) [EDPBI:LU:OSS:D:2021:240][47] or this information was provided with delay.[48]

With regard to the controller's obligation to inform the data subject about the action taken on the requests received (Art. 12(3) GDPR), the case law considered has also clarified that, when the controller notifies the data subject that the request has been granted, the erasure has been initiated and how long it will take at most, no confirmation that the erasure had been carried out is required. This is unless the data subject requests otherwise, or it is indicated that the data subject wishes to be notified that the erasure has been carried out or that the erasure is not carried out within the specified time limit [EDPBI:SE:OSS:D:2021:303].

As regards **human errors**, they may concern requests inadvertently not processed or not forwarded to the competent department [EDPBI:DEBE:OSS:D:2020:130; EDPBI:CY:OSS:D:2021:267], as well as occasional misclassification of the data subject's requests [EDPBI:DEBE:OSS:D:2021:184; EDPBI:SE:OSS:D:2021:195] or misrepresentation of the data subject's position.[49]

---

[43] See also EDPBI:DEBE:OSS:D:2018:10 in a case where the erasure request was not handled in a timely manner as there were two separate databases, managed by the customer care and the in-house shop management, and the account was deactivated on the former, but the request was not forwarded to the shop management.

[44] See also EDPBI:CZ:OSS:D:2021:312; EDPBI:FR:OSS:D:2020:105.

[45] See also e.g. EDPBI:CY:OSS:D:2021:305 in a case of an oral request for erasure, where the LSA emphasised that both the data controller and the provider must facilitate the exercise of the right of erasure by properly training their employees and, as far as the controller is concerned, adopting clear instructions on the handling of the erasure requests; and EDPBI:DEBE:OSS:D:2021:374 in a case where the data processor treated a data subject's request internally instead of forwarding it to the controller, as required by the nature of the service and task allocation.

[46] See also EDPBI:FR:OSS:D:2020:193 where the data subject's request for erasure was addressed by assigning personal information a special status making then unusable by the data subject, but without erasing them from the database.

[47] See also EDPBI:DEBE:OSS:D:2020:156, see also EDPBI:FR:OSS:D:2020:84.

[48] See also EDPBI:HU:OSS:D:2020:118.

[49] See also EDPBI:PL:OSS:D:2020:194, in a case of wrongful compliance with the data subject's request for erasure due to lack of the information on one of the several active processing operations concerning the data subject.

In addition, a combination of procedural and human errors is likely to occur in the case of erasure r**equests handled manually and not via digital communications and automated procedures**.[50]

Based on the case law of the LSAs and in the light of the EDPB guidelines,[51] data controllers are required to ensure the effectiveness of all data subjects' requests concerning the exercise the right of erasure, and personal data must be systematically erased when requested.

Against this background, the automation of the complaint process can reduce both the procedural and human errors, by introducing user-friendly interfaces that support data subjects in formulating and providing better evidence of their requests, and by setting the decision-making process regarding erasure so as to be aligned with the tasks assigned under the GDPR to those handling personal data. This ensures more effective compliance with both the data subjects' requests and the GDPR, without prejudice to the human decision on each case, which remains in the hands of the persons tasked by the controller to make the final decision. In the most basic cases, such as erasure resulting from contract/service termination, full automation may be considered.

6.1.3.2.4. OVERRIDING LEGITIMATE INTEREST AND OTHER CONDITIONS JUSTIFYING DATA PROCESSING DESPITE A REQUEST FOR ERASURE

More complicated issues, entailing a case-by-case assessment and the involvement of a human decision-maker, arise in cases where the request for erasure cannot be accepted due to the presence of overriding legitimate grounds for the processing (Art. 17(1)(c) GDPR), or where the right to erasure is not granted when processing is necessary under Art. 17(3) GDPR.

As to the first category of cases, they mostly deal with the prevalence of data **controllers' legitimate interest** [e.g. EDPBI:SE:OSS:D:2021:196 where the data subject's right to the erasure of banking information did not override the legitimate interest of the data controller in payment and fraud prevention, in a case involving the use of unique payment instrument identifiers to counter the abuse of free trial online services offered by a media company]. In this regard, it is worth noting that the decisions examined do not include cases of the exercise of right to be forgotten in the context of the activity of search engines, which are instead common in national and regional decisions of individual Supervisory Authorities.

Regarding the second category, i.e. cases where the right to erasure is not granted, the LSA decisions mainly concern **obligations under national laws** setting mandatory data retention periods [e.g., EDPBI:DK:OSS:D:2021:210 data retention required by the law with regard to customers' complaints and purchases].[52] Data controllers must **inform data subjects about the legal grounds** for retaining their data, which justifies the rejection of any erasure request [EDPBI:MT:OSS:D:2022:340, regarding anti-money laundering obligations; EDPBI:MT:OSS:D:2021:272, concerning various obligations under banking laws]. In these cases, **specific information on the source of the legal obligations** must also be provided to the data subject at the time of the request for erasure (Article 12.1) [EDPBI:MT:OSS:D:2021:272].

[50] EDPBI:SE:OSS:D:2021:178 in a case where the data subject was not informed about the results of the erasure request, as the request was handled manually, because it was received by mail, whereas the company used to handle requests through an automated digital system where notifications about measures taken were sent automatically.

[51] See Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, available at https://ec.europa.eu/newsroom/article29/items/611237/en, accessed 10.10.2022, 12; "[…] failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence".

[52] See also CJEU, case C-398/15, Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni.

However, **legal obligations must be interpreted in line with data protection principles** and not abused to justify limitations to the rights of the data subject. In this sense, for example, the consumer's right to claim compensation for a defective product for two years after the delivery of the goods to the purchaser cannot justify a refusal to erase a customer's profile because of the use of an online form on the customer's page to exercise the right to complain, as it is possible to complain about a product in a different way with no need to maintain an active profile.[53]

Legal obligations and the defence of legal claims (Art. 17(3)(e) GDPR) related to consumer protection may also justify the retention of personal data processed in connection with orders during the time when purchasers may make their claims, or a competent supervisory body may carry out an inspection [EDPBI:CZ:OSS:D:2021:312].

Nonetheless, it is worth emphasising that, while under certain circumstances some personal data may be kept in intermediate storage in the presence of an erasure request, those that are not necessary in the context of fulfilment of such obligations or purposes under Art. 17 GDPR must be deleted after the exercise of this right [EDPBI:FR:OSS:D:2021:279; EDPBI:FR:OSS:D:2021:310].

6.1.3.3. CONCLUDING REMARKS

Due to the nature of the cases decided, most of the complaints relating to Arts. 17 and 21 GDPR concern minor violations and are often characterised by a collaborative approach on the part of the data controller, with spontaneous remediation of the infringement, including the adoption of new procedures fully compliant with the GDPR.

For this reason, discontinuation of data processing and erasure of personal data as a result of LSA investigations and active cooperation by data controllers make reprimands the main outcome in the case law examined. It is worth noting that, in presence of minor violations, the motivation of the remedy adopted in the final decision is sometimes quite brief, by using general statements (see e.g., EDPBI:DEBE:OSS:D:2021:184 which refers to "the specific circumstances of the case under investigation").

Although in some cases the LSAs have imposed specific sanctions on data controllers, this is usually due to a large number of infringements of the GDPR, with a minor role played by violations of Arts. 17 and 21 GDPR. This also makes it difficult to identify in the Register a set of notable case studies focusing on these specific legal grounds.

Finally, it is worth noting that even where the violations of Art. 17 GDPR are more serious, the LSAs may consider refraining from imposing a fine in consideration of the specific circumstances of the case [e.g. EDPBI:DEBW:OSS:D:2021:203 where the LSA took the following elements into account: "First of all, it must be seen that [the data controller] is a non-profit and thus not commercially active company which, apart from the managing sole shareholder, has no employees and is dependent on donations for its non-profit activities, which in 2020 amounted to only EUR 10,603.00 up to the time of the statement of 24 November 2020. In addition, did not act intentionally, but on the contrary, due to a lack of technical expertise, was convinced that the signature list had already been deleted and had thus complied with the complainant's request for erasure".

6.1.4. MUTUAL ASSISTANCE

The mutual assistance procedure allows SAs to ask for information from other SAs or to request other measures for effective cooperation, such as requests

[53] See also EDPBI:DK:OSS:D:2020:171 and EDPBI:DK:OSS:D:2021:210 where it was deemed unnecessary to keep the customer account active for at least two years after the purchase for the exercise the right to complain under the customer protection law, as this right can be exercised by other means such as emails or telephone.

to carry out prior authorisations and consultations, inspections and investigations. Mutual assistance can be used for cross-border cases subject to the OSS procedure, either as part of the preliminary phase, to gather the necessary information before drafting a decision, or for national cases with a cross-border component.

The IMI enables the use of either informal mutual assistance without any legal deadline (voluntary mutual assistance) or the use of formal mutual assistance. In the latter case, according to the GDPR, the SA from which information has been requested has a legal deadline of one month to reply.

Between 1 January 2022 and 31 December 2022, SAs initiated 248 formal mutual assistance procedures and 2924 voluntary mutual assistance procedures.

6.1.5. JOINT OPERATIONS

The GDPR allows SAs to carry out joint investigations and joint enforcement measures. Similar to the Mutual Assistance procedure, SAs can use joint operations in the context of cross-border cases subject to the OSS procedure, or for national cases with a cross-border component.

In 2022, SAs did not carry out any joint operation.

6.2. NATIONAL CASES

SAs have different investigative, advisory and corrective measures at their disposal to ensure entities within their countries apply data protection law correctly and consistently. Corrective measures include the following:

- Issuing warnings to a controller or processor where its intended processing operations are likely to infringe the GDPR;
- Issuing reprimands to a controller or processor where processing operations have infringed the GDPR;
- Ordering the controller or processor to comply with a data subject's request or to bring processing operations into compliance with the GDPR;
- Imposing processing limitations, bans or fines.

6.2.1. SOME RELEVANT NATIONAL CASES WITH EXERCISE OF CORRECTIVE POWERS[54]

SAs play a key role in safeguarding individuals' data protection rights. They can do this by exercising corrective powers. The EDPB website includes a selection of SA supervisory actions. This section of the Annual Report contains a non-exhaustive list of certain national enforcement actions in different EEA countries carried out outside the OSS cooperation mechanism.

The cases examined in this section highlighted a lack of proper technical and organisational measures for processing personal data securely, which led to data breaches. Several other cases revolved around data processing without a data subject's consent. Some significant incidents also involved the unlawful processing of special categories of personal data, such as health data. Moreover, numerous cases involved data subjects who could not effectively exercise their rights, such as the right of access, the right to erasure and the right to object to data processing. Finally, a great number of cases also included the controller's failure to notify the data subjects of the occurred or the potential risk of data breaches. Entities from both the private and public sectors were fined by the national SA.

[54] This selection of enforcement actions only includes those that were sent to the EDPB by the SAs following a request to submit national enforcement news. Further cases can be found on https://edpb.europa.eu/news/news_en.

6.2.1.1. BELGIUM

In 2022, the Belgian SA investigated several complaints and discovered violations by data controllers on issues related to, among others, security of processing, sensitive data, consent, transparency, cookies, thermal cameras and COVID-19.

In April, there were two cases worth highlighting. In the first one, the Belgian SA established that the controllers, Brussels Airport and Ambuce Rescue team, did not have a valid legal basis under Arts. 6(1) and 9(2) GDPR for carrying out temperature checks on passengers and for the processing of special categories of personal data (health data) in the context of the COVID-19 crisis. Moreover, one of the controllers infringed Arts. 12 to 14 GDPR due to a lack of transparency vis-à-vis the data subjects. Administrative fines of respectively EUR 200,000 and EUR 20,000 were imposed by the Litigation Chamber on the controllers. Later, the Market Court of Brussels (Court of Appeal) reduced the fine imposed by the Belgian SA on Brussels Airport to EUR 50,000 and cancelled the fine imposed on Ambuce Rescue Team.

The second case concerned the use of thermal cameras at Brussels South Charleroi Airport to check, in the context of COVID-19, whether the passengers had a body temperature of 38 degrees Celsius or above. In this regard, the Belgium Litigation Chamber held that the airport lacked a valid legal basis for processing data related to the temperature of travellers, particularly considering it processed data pertaining to a special category under the GDPR (health data). Additionally, the Belgian SA observed shortcomings in terms of purpose limitation, transparency and the information provided to travellers, as well as in the quality of the Data Protection Impact Assessment (DPIA) and the record of processing activities. As a result, the airport was issued a EUR 100,000 fine, which was later reduced by the Court of Appeal to EUR 25,000.

On 4 May 2022, a complaint was filed against the NMBS/SNCB in relation to the company's Hello Belgium Railpass, which was issued free of charge to Belgian residents during the COVID-19 crisis. It was revealed by a Twitter user that the newsletter providing information on the Railpass did not contain a possibility to unsubscribe. The Belgian SA argued that the Railpass could not be classified as a "communication from public authorities" or a "promotion at the initiative of public authorities" and as such had no legal basis under Art. 6(1)(e) and (f) GDPR. Indeed, while the controller could inform customers about COVID-related measures, it could not promote trips to tourist sites. Moreover, the newsletter did not provide an indication of the possibility to object which is a right guaranteed in Art. 21(2) GDPR. Thereby, the Litigation Chamber of the Belgian SA decided to impose a fine of EUR 10,000 on the NMBS/SNCB.

Later in May, two cases were addressed by the Belgian SA. The first case related to a complaint filed against the websites sos-services.be and sos-avocats.com. According to the plaintiff, these websites, operated by the same controller, listed lawyers and other professionals without valid legal basis and without the lawyers being informed about the processing of their personal data. Additionally, the plaintiff argued that the information was erroneous and that testimonies were falsely attributed to the listed lawyers. In addition, a lack of compliance with the GDPR of the privacy and cookie policy on the two websites was also raised. The Belgian SA imposed a fine of EUR 5,000 on the controller and ordered that the processing of personal data related to the lawyers be stopped and the data be deleted. It also ordered the controller to submit within three months a revised and compliant cookie and privacy policy to the Belgian SA's Litigation Chamber.

In the second case, a press website named the Roularta group was imposed a fine of EUR 50,000 by the

Belgian SA's Litigation Chamber for failure to meet the necessary conditions for valid consent, in the context of the processing of personal data on its websites. It was established that several cookies were placed by these websites on the user's device even before the user had given his consent and that the group had failed to comply with the obligation to provide information to users in a transparent, understandable and easily accessible form. Additionally, the consent boxes for the installation of cookies by third-party partners were pre-ticked, while consent must be the result of an active action.

As a result of a thematic inquiry into the installation of cookies by the most popular Belgian press websites, a second decision was made against another Belgian press website, "the Rossel group", on 16 June 2022. Shortcomings were found by the Belgian SA in terms of the consent required for the placement of non-essential cookies, namely: prior consent, absence of consent for audience measurement and social network cookies, lack of information to the users, further browsing as well as pre-checked consent boxes. The Rossel group was fined EUR 50,000 and ordered to bring the processing of personal data in line with the provisions of the GDPR.

In July, the disclosure by the Belgian public administration of information regarding the health status of their employee, hereby the complainant, was deemed by the Belgian SA as not compatible with the principle of data minimisation. Indeed, according to Art. 5(1)(c) GDPR only certain employees, exercising specific functions are entitled to receive this information. However, in this case, the health status of the complainant was disclosed via the minutes of the staff meeting, thereby pursuing an objective distinct from the original purpose, which was for the administration to receive and process this information in its capacity as an employer. In order to prevent similar incidents from happening again, the Litigation Chamber reprimanded the Belgian public administration and urged it to raise awareness among its staff members.

Finally, in August, the Belgian SA dealt with a case concerning security of processing. A company that developed a digital administration platform failed to implement the necessary security measures. Indeed, it did not consider the risks that are presented by processing data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. As a result, the controller was issued a fine of EUR 2,500.

6.2.1.2. BULGARIA

The Bulgarian SA, the Commission for Personal Data Protection (CPDP), dealt with many cases in 2022. This section covers four noteworthy decisions related to the following topics: security of processing, illegal processing and dissemination, consent, public interest and sensitive data.

In October, a notification was received by the CPDP about a violation of personal data security due to non-functioning software applications at "Bulgarian Post" EAD. As a result of a subsequent inspection, it was revealed that when carrying out its activities as a personal data controller, the "Bulgarian Post" EAD did not apply sufficient technical and organisational measures. As a result of which, unauthorised disclosure of individuals' personal data was gained to the maintained information databases. Due to the unauthorised access of data by hackers, the ability to guarantee permanent confidentiality, availability, integrity and sustainability of processing systems and services was violated, as well as the ability to promptly restore access to the personal data. A sanction in the amount of BGN 700,000 (approximately EUR 358,098) was therefore imposed by the CPDP on the "Bulgarian Post" EAD for infringing Art. 32(1)(b)(c) and (d) GDPR, as well as Art. 32(2) GDPR, in connection with Art. 5(1)(f) GDPR.

Two other cases of interest were dealt with in December 2022. The first one concerned a complaint filed against a credit institution (bank), with allegations of unlawful processing of the complainant's personal data for direct marketing purposes. The CPDP argued that the email sent to the complainant, after he had terminated his relationship with the bank, regarding an offer for a "fully digital" consumer loan was not appropriate. Indeed, the bank was unable to guarantee and prove that the processing of the complainant's personal data for marketing purposes was carried out in accordance with the GDPR, which is the obligation of the controller under Art. 24 GDPR. The bank was consequently reprimanded by the CPDP and took active steps to ensure that the status of customers who have terminated their relations with the bank, will be marked from "active to "inactive" immediately after closing an account with the company.

A complaint was also filed in December by a Member of the Bulgarian Parliament with allegations of illegal dissemination on national media of data related to his health, specifically his vaccination status in the context of COVID-19. While the complainant disputed that his vaccination status was aired without his consent, the CPDP held that the processing of his personal data was lawful. Indeed, the CPDP based its decision on the argument that the person's consent is not an element of the lawfulness of personal data processing for journalistic purposes. Furthermore, the CPDP argued that the processing was carried out for the fulfilment of freedom of expression and the right to information in a democratic community.

Lastly, an ongoing case regarding the processing of personal data of deceased individuals by political parties during the national representative elections of October 2022, was opened by the CPDP in August 2022. For the time being, the CPDP established that eight political entities processed without a legal basis and in violation of the public interest, the data of less than ten deceased persons in their respective voter lists. It remains to be seen how the CPDP will handle these administrative violations in its final decision.

6.2.1.3. CYPRUS

The Cyprus SA handled several cases in 2022 involving, amongst others: a journalistic article for a politically exposed person, data breach of a school's emailing tool, data breach notification by a bank and the incorrect delivery of an application form.

The first case of interest involved a failure to comply with the principles of lawfulness, fairness and transparency, data minimisation and the principle of accuracy (Arts. 5(1)(a), (c) and (d) GDPR). The Cyprus SA issued an administrative fine of EUR 10,000 to the controller in February for having published an article containing inaccurate details about the complainant's financial status, simply to satisfy the public's curiosity. The complainant was ordered to remove the relevant article from the web pages he controlled within a week.

In March, the Cyprus SA imposed two fines, one of EUR 5,000 and the other amounting to EUR 4,000, on two separate entities. The case pertained to the unauthorised usage of a school's email tool by the president of a teacher's trade union (TU). The president sent an email to all the parents of the students, using their email addresses, for trade union purposes. In doing so, the president of the TU acted as a separate controller and therefore the TU was fined for his actions. The second fine was imposed on the school for lack of appropriate technical and organisational measures to prevent the processing of email addresses by teachers, for purposes other than schooling.

Another fine was issued by the Cyprus SA in July 2022 for the infringement of the principle of integrity and confidentiality (Art. 5(1)(f) GDPR) as well as the lack of technical and organisational measures on behalf of the controller (Arts. 24(1) and 32 GDPR). The

controller in this case was a bank that was involved in three separate data breaches and as a result, was fined EUR 17,000. In the first breach, a letter addressed to a bank's customer was sent to another company, and in the second, 11,673 electronic files belonging to bank customers were accidentally sent to the same organisation. The third incident involved sending the company one electronic file which contained notice letters the bank had sent to its customers. In total, 8,500 data subjects were affected by these incidents.

The last case concerned the same infringements as the case mentioned beforehand. Indeed, in September 2022, the Electricity Authority of Cyprus (CEA) was fined EUR 5,000 by the Cyprus SA for unlawfully disclosing personal data concerning the complainant to a third party. More specifically, an application form for installing a power line, that should have been delivered to the complainant for signature, was delivered instead to his neighbour, by a CEA employee. The application form contained personal data of the complainant and it was established that the CEA employee had untruthfully signed the form that he had personally delivered to the complainant.

6.2.1.4. CZECH REPUBLIC

In 2022, the Czech SA fined a controller CZK 70,000 (EUR 2,800) for processing personal data without legal ground. The SA stated that the controller misled data subjects freshly registered with the Trade Register by offering them entry into the private and paid "Registry of Commerce and Trade", which they were ultimately prompted to pay for. As a result thereof, the controller processed the name, surname, business address, and company identification number of data subjects retrieved from the Trade Register. Although the controller processed the data which was publicly accessible in the Trade Register, the Czech SA ruled that it was not permissible to process such data freely without any legal basis.

6.2.1.5. DENMARK

In most EEA jurisdictions, SAs have the power to issue administrative fines themselves. In Denmark, however, this is not the case. Indeed, data protection law infringements are first looked into by the Danish SA before being reported to the police. After the police has conducted an investigation to determine whether charges should be filed, the court then decides on any possible fines.

In January, the Danish SA expressed serious criticism against controller Den Blå Avis for the processing of personal data of individuals visiting its website. Particularly, it was established that the controller's consent mechanism on its website did not meet the legal criteria for a valid consent. Moreover, the processing, which was conducted for analytical and statistical purposes, did not respect the core principles of the GDPR such as lawfulness, fairness and transparency.

In March, the Danish Municipality was reprimanded for revealing by email confidential health information about one of its employees. Indeed, the complainant's colleagues were notified by the municipality that the woman could no longer conduct challenging physical tasks, due to her ongoing fertility treatment. In its decision to reprimand the municipality, the Danish SA emphasized a great deal on the sensitive nature of the data which had been shared with the group of people.

In April, the Danish Financial Supervisory Authority was seriously reprimanded by the Danish SA for violating the requirement of adequate security when processing data (Art. 32(1) GDPR). The controller mistakenly supplied information regarding whistle-blowers to a journalist in connection with a request for document access. Indeed, the personal data contained in the file was not successfully erased by the controller, rendering it possible for the journalist to access it. In this case, the Danish SA emphasised that in situations where the data originates from a system of whistle-

blowers, the risk of violating the rights of data subjects is greater.

In May, the Danish SA issued a decision in regard to a case concerning the use of an AI-profiling tool "Asta" by municipal authorities. The tool was used by the authorities to determine the length of the contact process between a newly unemployed person and the unemployment centre. However, this was estimated by processing data from unemployed persons and comparing it to the value of created (generic) individuals. The Danish SA came to the conclusion that an unemployed individual's consent does not constitute a legal basis for the processing of his personal data. It particularly highlighted that in the context at hand, consent cannot be considered to have been given freely.

In June, a request was made by a data subject for access to documents related to a pending court case. However, the complainant did not specify which documents were to be reviewed by the controller to identify personal data related to him. In its final decision, the Danish SA argued that this request did not entail an obligation for the controller to search for and review the documents in order to identify and provide information about the data subject.

In October, an issue related to consent was brought to the attention of the Danish SA. The case concerned the processing of personal data of visitors to a Danish website. In its decision, the Danish SA considered that the controller of the website, JP/Politiken, failed to provide information to the visitors about the purposes of data processing. Hence, it could not be agreed that the visitors had given informed consent. Additionally, the Danish SA argued that the "accept all" option of the consent mechanism set in place by the controller conflicted with the principle of lawfulness, fairness and transparency. As a result, the Danish SA reprimanded JP/Politiken.

Several cases related to the processing of personal data of alleged victims and individuals accused of sexual harassment were dealt with by the Danish SA in February, September and November 2022. Regarding the lawfulness of processing, the Danish SA found that a general legitimate interest exists when investigating instances of sexual harassment. It thereby argued that the controllers could process the data based on several provisions of the GDPR, namely Art. 6(1)(f), Art. 6(1)(e) or Art. 9(2)(f). However, due to a lack of information provided to the data subjects regarding the processing of their personal data, the Danish SA issued reprimands to the controllers.

6.2.1.6. ESTONIA

Upon conducting, on its own initiative, a monitoring operation of the Facebook groups that publish personal data of individuals in debt, the Estonian SA issued a decision in January 2022 against the controller. The controller, who held the position of administrator of the Facebook groups, stated that the processing was done for personal purposes. However, the Estonian SA argued this not to be true, since the groups were composed of a number of members between 4600 and 14,800, thereby entailing that the data was disclosed to an unidentified group of individuals. Ultimately, the Estonian SA recalled that the processing of information related to the financial status of individuals would infringe on their rights. The controller was issued a fine of EUR 5,000 and was requested to stop sharing individuals' personal data in Facebook groups without their explicit consent.

The same month, the Estonian SA issued a precept with a penalty payment of EUR 10,000 on the controller Krediidiregister OÜ for each unfulfilled obligation. It requested the controller, amongst other obligations, to terminate the disclosure of all valid and invalid data of natural persons related to a legal identity. Moreover, the controller was ordered to verify that third parties who received the data had a legitimate interest.

On 25 July 2022, the Estonian SA ordered the controller Ticketer OÜ to (i) align its privacy notice

with the requirements set in the GDPR and (ii) either remove the website's third-party cookies or obtain consent from the data subjects before placing the cookies. The decision of the Estonian SA resulted from a self-initiated monitoring operation to assess the way personal data is processed in various ticket seller portals. During the operation, it was revealed that the controller's website lacked a privacy notice as well as other GDPR requirements, such as a purpose and a legal basis for processing. The Estonian SA issued a precept with a penalty payment of EUR 5,000 for each unfulfilled point.

6.2.1.7. FINLAND

In this section, seven cases from the Finnish SA's work related to data protection violations will be presented.

On the basis of non-compliance with an order issued by the Finnish SA, a telemarketing company was awarded an administrative fine of EUR 8,300 on 29 April 2022. The Finish SA decided that the controller had failed to comply with its order to fulfil a customer's request to access the recording of a sales call. Having access to the recording would have enabled the customer to identify whether the telemarketing company's methods for promoting and selling its goods to older customers had been legal.

In response to the eleven cases brought to the SA concerning Otavamedia Oy, the Finnish SA adopted a decision against the controller in May 2022. Complainants criticised the controller for ignoring their requests concerning data protection rights. However, the controller shed light on a technical issue that prevented the data protection requests from being directed to customer service. Nevertheless, the Finish SA noted the controller's responsibility to ensure the functionality of the email inbox, especially as it was the main contact channel for data protection matters. Furthermore, the SA found that Otavamedia Oy had gathered a considerable amount of identification data (i.e. complainants' signatures) by imposing the use of a printable form for data protection requests. Consequently, the controller was ordered to update its processes to comply with the requirements for data protection and was issued a fine of EUR 85,000.

On 8 June 2022, the Finish SA ordered three insurance companies to correct their activities related to the processing of health information of insurance applicants. This was ordered to ensure that future processing activities would comply with the GDPR. One of the insurance companies was notably reprimanded by the SA as it requested consent for processing health data without properly identifying the purposes behind the use of this data. Furthermore, it was revealed that the insurance companies were not clear as to whether they only limited their data requests to health information deemed necessary for assessing the liability of the company.

Later in July, the Finnish SA issued a reprimand to a bank for its failure to enable their customers' inquiry into the erasure of their personal data. The Ombudsman strongly believed that such data should have been erased and if not, the reasons for keeping it should have been communicated to the customers. The Finish SA also reprimanded the controller for erasing one of the complainant's data before the customer had been able to access it. It emphasised that in cases where a data subject wants to both access and delete personal data, then the request to access it should be completed first.

In October, the Legal Register Centre was warned by the Finish SA that its planned processing of personal data would likely infringe the GDPR. The Finish SA based its decision on the fact that the controller was unable to reduce the risks inherent to the planned processing measures. This included a risk that the data would be transferred to non-EU countries' authorities, as a result of their right of access to information.

In November, the Finish SA issued a reprimand against the Tax Administration for the failure to fully consider

the risks involved in processing personal data. Indeed, between 2015 and 2021 the controller issued requests for information regarding all cross-border credit transfers, which included data on banks' customer registers. However, the controller only limited the transactions to be investigated after having the data in its possession, and as a result, infringed the GDPR.

After having received three complaints from private individuals, the Finnish SA opened an investigation into the controller Alektum Oy. It was revealed that the controller had not only failed to give a reply to the individuals' requests to access their personal data, but also purposely delayed the investigation by avoiding the Finnish SA. In addition to being reprimanded by the SA in December 2022, the controller received a fine of EUR 750,000 for seriously violating data protection rules.

6.2.1.8. FRANCE

In 2022, France handled several cases where it issued considerably large fines. This section will present a selection of those cases.

A significant fine was first issued to a controller in April 2022. The fine amounted to EUR 1,500,000 and was served to Dedalus Biologie by the French SA regarding a massive data breach of the personal data of 500,000 people. In this case, sensitive information about the individuals' health as well as their name, social security number, name of prescribing doctor and date of examination, was released on the internet. The French SA held that the compromised data was a direct consequence of the controller's lack of satisfactory security measures.

On 23 June, TotalEnergies Électricité et Gaz France was issued a sanction of EUR 1,000,000. The French SA accused the controller of rendering it impossible for individuals to refuse commercial prospecting. When filling out a web form for subscribing to an emerging contract, the user had no means to refuse the re-use of their personal data for ulterior purposes, such as commercial canvassing. In doing so, the controller infringed several provisions of the GDPR, notably the obligation to inform solicited individuals, the right of access to data and the right to object of data subjects, as well as the obligations relating to the modalities for exercising rights.

On 19 October, the controller Clearview AI was subjected to a maximum financial penalty of EUR 20,000,000. French SA issued the fine as a consequence of the controller's failure to comply with the SA's earlier formal notice. The formal notice ordered the controller to stop the collection and use of the data of French citizens without a legal basis and to comply with their requests for erasure. In light of the serious violations of the data subjects' fundamental rights, the restricted committee added to the fine a penalty of EUR 100,000 per day for delay in complying with the order.

In November, three interesting cases were handled by the French SA. On 10 November, the controller Discord Inc was issued a hefty fine of EUR 800,000 for having infringed several provisions of the GDPR. This included a failure to define and respect a data retention period appropriate to the purpose of processing data (Art. 5(1)(e) GDPR), to comply with the requirement of providing information to the data subjects (Art. 13 GDPR), to ensure data protection by default (Art. 25(2) GDPR), ensure personal data security (Art. 32 GDPR) as well as a failure to perform a DPIA (Art. 35 GDPR).

Later in the month, the main electric utility in France "EDF" was held accountable for omitting to consider the data rights of its customers. Indeed, the controller did not collect the consent of individuals to receive commercial emails, nor did it inform the customers about its data processing activities. Lastly, the French SA argued that EDF had failed to ensure the security of the personal data of the customers. For the reasons mentioned above, EDF was issued a fine of EUR 600,000.

Finally, the third case handled in November by the French SA concerned the challenges faced by individuals in having their requests for accessing or erasing their personal data considered by the controller Free. In addition to preventing individuals from exercising their rights to have access to their data or have it erased, the French phone operator Free failed to ensure the security of the data. The French SA established that the controller did not fulfil its obligation to document a personal data breach under Art. 33 GDPR. Free was therefore issued a fine of EUR 300,000 and ordered to comply with the requests of its customers within three months.

6.2.1.9. GERMANY

There are both national (federal) and regional SAs in Germany.

A case was handled by the SA of the Free Hanseatic City of Bremen in March 2022, regarding the processing by a large company of over 9,500 data. This data belonged to numerous prospective tenants and was processed by the controller without a legal basis. Moreover, the information processed constituted sensitive data specifically protected under the GDPR, such as skin colour, ethnic origin and religious affiliation. Additionally, it was discovered that the company had deliberately refused requests for transparency regarding its data processing activities. Considering the serious infringement of several provisions of the GDPR, the controller was issued three administrative fines of EUR 1,435,750, EUR 400,000 and EUR 75,000 respectively.

The same month, a second case related to the processing of personal data revealing political opinions was dealt with by the SA of the Free Hanseatic City of Bremen. In this case, a small regional political party went against the warning originally issued by the SA and proceeded to run a web-portal enabling students and parents to complain about the political views of teachers. As a consequence of having ignored the SA's warning and subsequently infringing the GDPR, the controller was issued a fine of EUR 6,000.

In August 2022, Berlin SA issued a fine of EUR 525,000 on a subsidiary of a Berlin-based e-commerce company. The SA concluded that the controller did not honour the reprimand issued against the company in 2021. Indeed, an inspection conducted by the Berlin SA in 2022 revealed that the controller had still not fulfilled its task to monitor the compliance of his service companies with data protection regulations.

6.2.1.10. GREECE

In a national case before the Hellenic SA, two mobile telecommunications companies were fined in January 2022 for personal data breaches. As a result of having provided unclear and insufficient information to its subscribers, the controller Cosmote was fined EUR 6,000,000 for infringing the principles of legality and transparency. Additionally, the Hellenic SA established that the company had taken inadequate security measures and, amongst other things, conducted a poor DPIA. The other controller, Ote, was also found guilty of infringing data security principles and received a fine of EUR 3,250,000.

In another case, the Hellenic SA issued a EUR 2,000 fine to a controller for the violation of individuals' rights to object, as well as the infringement of the GDPR principles of lawfulness, fairness and transparency. This fine was issued in March 2022 after a complaint was made by a teacher that their employer regularly monitored online courses taught via "Zoom", despite the employee's objections. Furthermore, the employer failed to provide a valid legal basis for the processing in question.

On 19 July 2022, the Hellenic SA dealt with a case of unlawful processing of data revealing the balance of a debtor's debt. The processing was conducted by a loans and credits claims management company even though a judicial exemption from the complainant's

debts existed. Furthermore, by claiming that the complainant could not be identified, the controller impeded the exercise of their rights. Hence, the Hellenic SA decided to impose two fines of EUR 10,000 each on the controller for the various GDPR infringements.

A second decision was adopted by the Hellenic SA in July 2022. This decision was issued against Clearview AI Inc, a company marketing facial recognition services, for violating the principles of lawfulness and transparency. The company received a EUR 20,000,000 fine and was ordered to satisfy the complainant's request for access to personal data. Additionally, the Hellenic SA commanded the controller to delete all personal data of the Greek data subjects which it had processed using facial recognition technology. A general prohibition to process personal data using such methods was also imposed on the company.

In August, several controllers were issued fines in a case involving the publishing and processing of the results of self-tests on the electronic application "self-testing.gov.gr". Indika S.A. was fined EUR 5,000 for the lack of effective security measures, while the controller, Greek Seamen's Fund (NAT), was ordered to remove the application from its IT system as well as delete the data of ship crew members. Moreover, Indika S.A. and the Ministry of Labour and Social Affairs were reprimanded for drafting an incomplete and overdue impact assessment. Finally, a fine of EUR 5,000 was issued to both the Ministry of Interior and NAT for omitting to comply with the requirement to carry out an impact assessment.

6.2.1.11. HUNGARY

In 2022, the Hungarian SA imposed multiple fines for violations of data protection law. Selected cases are listed here:

- In February, the controller Budapest Bank Zrt was fined EUR 650,000 for processing, with the help of software using AI, the emotional state of its clients during calls. The Hungarian SA concluded that both the legitimate interest and impact assessments failed to provide any actual risk mitigation and that data processing using AI may pose a high risk to individuals' fundamental rights.
- In April, the Hungarian SA held that the Hungarian Two Tailed Dog Party, a political satirical joke party, had not applied sufficient security measures when storing the data of sympathisers and activists. Indeed, this special data was stored online on Google sheets, thereby rendering it possible for anyone with a link to access and download it on a local computer. A fine of EUR 7,500 was issued to the Party.
- In March, a serious case regarding the publication of pornographic photographs of a data subject on a website was handled by the Hungarian SA. Even though the complainant had given consent to be photographed 10 years ago, the SA argued that such consent was not a valid legal ground for the processing activities of the website's controller, especially since the pictures featured the complainant's full legal name. Not only was the processing held unlawful, but the controller also infringed the rights of the complainant by denying its request to have the data deleted. The SA thereby ordered the controller to erase the pictures and the subject's legal name from the website.
- In August, the Hungarian SA dealt with a national case involving the processing of personal data by a financial institution during credit assessments. In the case at hand, the complainant had not given their consent to have his personal data processed during such assessments. The controller was imposed a fine of approximately EUR 78,945 for failing to refer its processing activities to an appropriate legal basis and to

carry out an interest assessment. Moreover, adequate information had not been provided to the complainant regarding the processing and storage of their personal data.

- In October, the Hungarian SA recalled that data processing through a camera surveillance system during opening hours is unlawful, based on Section 38 of EDPB's Guidelines 3/2019. The SA held that the controller of the surveillance system not only processed the data without a valid legal basis, but also failed to adequately inform individuals of the processing activities.
- In July, a physician was fined EUR 1,500 by the Hungarian SA for failing to be transparent regarding its data processing undertakings. The SA established that a client of the physician was refused access to a copy of the documentation laying down the care provided to her during the medical consultation. Additionally, it was discovered that the physician failed his legal duty to upload the findings electronically and provided the patients with a privacy statement containing untrue information.
- In September, the Hungarian SA issued an administrative fine of EUR 75,000 to the controller Magyar Éremkibocsátó Kft. The controller was criticised for processing the personal data of its clients, despite having not received their informed consent. Indeed, when purchasing collectors' coins issued by the company, clients would have to check a box containing both the statement of purchase and the statement of consent to future marketing offers. The controller was therefore ordered by the SA to provide clear information to its customers.
- Later in the month of September, TV2 Média Csoport Zrt which operates two media websites was fined EUR 25,000 by the Hungarian SA. The fine was issued as a result of the controller's failure to solve the limitations of its cookie consent management systems (CMS). Indeed, the Hungarian SA held that the CMS did not comply with the GDPR.
- Lastly, an important case worth highlighting is the case related to the alleged use by the Hungarian law enforcement agencies and National Security Services of the spyware called "Pegasus" against investigative journalists and lawyers. On 9 August 2021, the Hungarian SA launched an investigation *ex officio* to assess whether the activities of the latter were compliant with data protection regulations. This investigation was launched after a list containing some 50,000 phone numbers, that had potentially been targeted by the surveillance tool, was leaked. In its decision, the Hungarian SA held that the processing of data with the surveillance tool Pegasus was in accordance with the relevant legal data protection regulations.

6.2.1.12. ICELAND

The Icelandic SA handled several cases in 2022, focusing mainly on the unlawful processing of personal data.

On 8 March, the Harpa Concert Hall and Conference Centre was ordered to stop processing the data present on the tickets purchased by individuals for events organised by the company, such as ID numbers and dates of birth. The Icelandic SA held that this processing was not necessary as the contract of the purchase could have been fulfilled without this data. As a result of having violated the principles of legality, fairness, transparency and minimisation of data, the company was fined ISK 1,000,000 (approximately EUR 7,200) and was further instructed to delete all the collected data.

On 3 May, the Icelandic SA issued a fine of ISK 1,500,000 (approximately EUR 10,700) on the controller HEI ehf, a medical travel agency in Iceland. The SA determined

that the controller had not established the lawfulness of the processing by its employee of several doctors' email addresses. Additionally, the complainant's right to access his personal data was infringed by the controller who deliberately erased the data before processing the request.

On the same day, 3 May, the Icelandic SA imposed a fine of ISK 5,000,000 (approximately EUR 35,768) on the municipality of Reykjavík for breaching several GDPR provisions by using Seesaw. It was established in a prior decision of the SA in December 2021, that the municipality was unlawfully processing the personal data of students using an American cloud-based service, Seesaw. The fine issued by the SA in 2022 was based on reasons stated in its first decision as well as the fact that the infringement concerned the processing of sensitive data (of children). Moreover, when calculating the fine, the Icelandic SA considered that the municipality had co-operated, that there was no indication that the violation had caused damage and that Seesaw's general information security seemed to be adequate.

6.2.1.13. IRELAND

As a result of a personal data breach involving the accidental publication of individuals' personal data on the internet, the Irish SA issued a reprimand and a fine of EUR 5,000 to Slane Credit Union Limited in January 2022. It was deemed that the controller had infringed the principle of security of processing laid down in Art. 5(1)(f) GDPR.

On 14 March, in a national case concerning the unauthorised disclosure and accidental alterations of customer personal data, the Bank of Ireland Group, a data controller, was issued a fine of EUR 463,000. Indeed, not only did the controller report the data breaches with undue delay, but it also provided insufficient information regarding the data breaches to the Irish SA. Additionally, the Irish SA established that the controller had failed to inform individuals in a timely manner that the breaches could potentially impact their fundamental rights and freedoms. Lastly, it was discovered that when transferring the data to the Central Credit Register, the bank had not ensured a level of security appropriate to the risks involved.

On 3 May, the Irish SA, of its own volition, conducted a monitoring exercise during which it evaluated whether public sector organisations were in compliance with the requirement to designate a data protection officer (DPO). It was established in this case, that the controller Pre-Hospital Emergency Care Council failed to designate a DPO and to publish and communicate the latter's contact details to the Irish SA. Consequently, the controller was issued a reprimand.

Furthermore, three important decisions were issued by the Irish SA in December 2022.

The Irish SA imposed a reprimand on the controller An Garda Síochána as it failed to implement appropriate technical and organisational measures when processing the personal data of 108 data subjects, some of whom were children. Moreover, the controller was ordered to bring its processing activities into compliance.

In a second case concerning the unauthorised access of a large amount of personal data, the Irish SA imposed a EUR 15,000 fine on the A&G Couriers Limited T/A Fastway Couriers Ireland. This sanction was issued in light of the controller's failure to provide a level of security suitable to the risks posed by its processing of personal data.

Lastly, the third decision issued in December by the Irish SA was made in relation to the illegal access by an unknown actor, most likely through a phishing attack, of personal data of residents of the Virtue Integrated Elder Care (VIEC). The Irish SA fined VIEC, as a controller, EUR 100,000 for failing to adopt appropriate technical and organisational measures which would have protected the data of its residents

and limited the risk of access to its email system where the data was processed.

6.2.1.14. LATVIA

On 21 April 2022, the Latvian SA, known as the Data State Inspectorate of Latvia, imposed an administrative fine of EUR 1,464.13 on the controller SIA "Your Move" for the infringement of Art. 83(5)(e) GDPR. The Latvian SA found that SIA "Your Move" had failed to comply with its order to provide information about the company's processing activities. In short, the SA ordered the company to provide an explanation regarding the personal data breach incident that took place on its website, however, the controller did not show an interest in providing the requested information. Hence, the controller failed to carry out its tasks under Art. 58(1)(e) GDPR.

6.2.1.15. LITHUANIA

The Lithuanian SA issued multiple fines in 2022. The Lithuanian SA carried out the following enforcement acts:

- Issued a fine of EUR 20,000 on a company providing credit assessment services for the processing of data on financial obligations, in breach of Art. 6(1) GDPR as well as Art. 5(1)(a) and (b) GDPR.
- Imposed a fine of EUR 6,000 on a company managing sports clubs for the failure to obtain the valid consent of its customers to process their biometric data. It was revealed that no alternatives for accessing the sports clubs other than identification through biometric data could be used by customers. In essence, the controller was fined for infringing numerous GDPR provisions, namely: principles of transparency and lawfulness (Art. 5(1)(a) GDPR), processing of special categories of personal data (Art. 9 GDPR), the right to be informed about the processing of personal data (Art. 13(1) and (2) GDPR), processing of activity records (Art. 30(1) and (3) GDPR) and Data Protection Impact Assessment (Art. 35(1) and (3)(b) GDPR).
- Issued a fine of EUR 35,000 on an IT company for its failure to ensure the ongoing confidentiality, integrity, availability and resilience of its data processing systems and services under Art. 32(1) (b) GDPR.
- Found an applicant's complaint concerning the disclosure of his residential address to be well-grounded. Indeed, the Lithuanian SA concluded that the controller, a public authority, had violated the principles of purpose limitation and data minimisation laid down in Art. 5(1)(b) and (c) GDPR by publishing the claimant's personal data.
- Decided that a controller's refusal to provide a client with a copy of the requested records of telephone conversations (which took place between the client and an employee) violated Art. 15(3) GDPR.
- Took corrective actions against a public organisation for infringing Arts. 5(1)(a), 6 and 7 GDPR. In this case, the Lithuania SA held that the controller had violated the GDPR by : (i) processing children's image data without their consent, (ii) failing to create the possibility of free choice and the inability to withdraw consent without suffering damage, and (iii) failing to give separate consent for individual operations of persona data processing.
- Recognised an applicant's complaint against a legal entity in the private sector as well-founded. The Lithuanian SA argued that the use by the controller of the complainant's personal correspondence with another employee, as a ground for dismissal, violated Art. 6(1) GDPR. No grounds could be used by the controller to justify that the processing was done in a lawful manner.

- Concluded that a controller infringed Arts. 5(1)(a) and 7(2) GDPR, as well as Art. 69(1) of the Law on Electronic Communications of the Republic of Lithuania by failing to acquire the applicant's legally compliant consent to receive direct marketing messages.

6.2.1.16. LUXEMBOURG

In March 2022, the Luxembourgish SA dealt with a complaint where a data controller did not fulfil its obligation to put in place appropriate security measures when processing personal data. The Luxembourgish SA solved this issue by reprimanding the controller and ordering him to comply with the provisions of the GDPR.

A month after, a data controller was found in violation of Arts. 13, 15 and 31 GDPR and was issued a fine amounting to EUR 1,500. Particularly worth mentioning is the controller's failure to respect the right of access of the complainant, by omitting to provide him adequate information as laid down in Art. 15 GDPR and its lack of cooperation with the SA.

Two cases involving the use of video surveillance for data processing purposes were dealt with by the Luxembourgish SA in 2022.

The first case concerned the use of video surveillance and geo-tracking systems to collect personal data, which was handled by the SA in February 2022. The data controller in this case was issued a fine of EUR 4,900. The Luxembourgish SA considered that the controller did not provide data subjects sufficient information regarding the processing of their personal data (Art. 13 GDPR) and that the ranges of cameras used were disproportionate to the objective pursued (Art. 5(1)(c) GDPR). Indeed, it was found that the controller had kept the personal data collected through the geo-tracking system for longer than necessary for the purposes for which it was processed.

The second case also touched upon the topic of data processing via a video surveillance system. The use of a total of twelve cameras by the controller was deemed disproportionate and in violation of Art. 5(1)(c) GDPR. Indeed, these cameras were aimed at the public road and neighbouring buildings, meaning that employees were constantly being monitored by the controller during both their worktime and break time. The controller was therefore issued a EUR 10,000 fine.

Finally in December, the Luxembourgish SA imposed a EUR 2,100 fine on a data controller for the failure to sufficiently inform data subjects (Art. 13 GDPR) and be transparent about its data processing activities (Art. 12(1) GDPR). According to the case facts, the controller collected personal data on its internet page as well as its mobile application.

6.2.1.17. THE NETHERLANDS

In 2022, the Dutch SA imposed multiple fines for GDPR violations. Three selected cases will be analysed in this section.

The first case concerns complaints made to the Dutch SA as to how the controller Sanoma Media Netherlands B.V. handled requests from individuals to access their data and have it deleted. Customers wishing to have their requests approved were asked by the controller to first provide a copy of their identity document, something which the SA deemed to be completely unnecessary. While DPG Media, the company that took over Sanoma, later changed its practice to ensure that the data subjects' rights would no longer be impeded, the Dutch SA however, still decided to impose a sanction. A fine of EUR 525,000 was issued to DPG Media.

The second case handled by the Dutch SA in 2022, involved the processing by the Ministry of Foreign Affairs of an average of 530,000 visa applications per year in the last three years. The main concern of the SA was the failure of the Ministry to sufficiently secure

the digital system it was using (NVIS) to process the data of visa applicants. Thereby, alongside a fine of EUR 565,000, the controller was ordered to adopt appropriate security measures in line with Art. 32(1) GDPR and provide applicants with adequate information about their data processed in the context of the Schengen visa process.

Lastly, in a third case concerning the use of a blacklist to register indications of fraud, the Dutch SA imposed a hefty fine of EUR 3,700,000 on the Tax Administration for illegally processing personal data for several years in its 'fraud identification facility'. The SA held that the use of the said blacklist by the Tax Administration greatly impacted the rights of individuals that were wrongfully added to it. Indeed, once included in this list, the individuals were registered as possible tax frauds.

6.2.1.18. NORWAY

The Norwegian SA carried out the following actions in 2022:

- Banned the processing of personal data of internet users by the controller Shinigami Eyes for failing to provide a legal basis for its processing activities. According to the SA, the controller which is a browser extension available for Chrome and Firefox, would tag individuals without their knowledge and in doing so would also give indications to other users as to whether the tagged individual was pro- or anti-trans. This subjective assessment was deemed by the SA to be a threat to the free exchange of ideas online.
- Issued a fine of EUR 5,000 on the controller Etterforsker1 Gruppen AS for performing an unwarranted credit rating on a private individual without any type of customer relationship between them.
- Imposed a hefty fine of EUR 500,000 on the Norwegian Labour and Welfare Administration for publishing CVs of users on the service arbeidsplassen.no without the proper legal basis to do so (Art. 6 GDPR). However, it is worth mentioning that the controller took active steps to remedy the situation when the infringement was discovered.
- Ordered the municipality of Østre Toten to implement a suitable control system for information security and personal data protection, but also imposed a fine of EUR 400,000 for the failure to protect its IT systems against a serious cyberattack. This attack was made possible due to the severe and fundamental security flaws present in its systems.
- Issued the controller Storting a fine of EUR 200,000 for inadequate security. Indeed, the Norwegian SA concluded that Storting had failed to prevent the unauthorised logins to important email accounts, such as those of parliamentary representatives, by not having implemented suitable technical and organisational measures as required under Art. 32 GDPR.
- Imposed a fine of EUR 500,000 to the controller Trumf for failing to secure the processing of its members' purchasing history. The SA held that the controller had not implemented a measure verifying whether a user registering a bank account was that account's real owner. Members of Trumf were therefore able to easily access the purchasing history of another individual by registering with the unknown person's account number.

6.2.1.19. POLAND

This section will highlight six cases of interest, handled by the Polish SA in 2022.

On 9 January, in a case involving the copy by unauthorized persons of an additional customer database of the controller, the Polish SA issued fines on both the controller and the processor. The controller,

Fortum Marketing and Sales Polska S.A, was issued a fine of EUR 1,080,000 for having infringed Arts. 5(1)(f), 24(1), 25(1), 28(1), 32(1) and (2) GDPR. The processor, however, was imposed a smaller fine of EUR 55,000 for violating Arts. 32(1) and (2) in relation to Arts. 28(3)(c) and (f) GDPR.

On 31 May 2022, the Polish SA issued an administrative fine of approximately EUR 2,200 on the Warsaw Centre for Intoxicated Persons for infringing, through its surveillance system, Art. 6(1) (lawfulness of processing) and Art. 5(1)(a) (principles of lawfulness, fairness and transparency) GDPR.

On 7 September, the Cultural Centre of Sułkowice municipality received an administrative fine of PLN 2,500 (approximately EUR 529) for outsourcing parts of its activities to a processor without a written contract, as required under Art. 28(3) and (9) GDPR. Furthermore, the controller failed to check that the processor had provided sufficient guarantees for the implementation of appropriate technical and organisational safeguards (Art. 28(1) GDPR).

On 2 November, the Mayor of the Commune was sanctioned for having infringed several provisions of the GDPR, namely: Arts. 25(1), 24(1), 5(1)(f) and (2), as well as 32(1) and (2). A fine of PLN 8,000 (approximately EUR 1, 695) was issued by the Polish SA to the Mayor after it was revealed that he had failed to implement security measures on its portable computer device. The computer, which was stolen as a result of a break-in in the controller's apartment, contained a file with personal data of the complainants.

On 16 November, the Polish SA issued a fine of EUR 340,717.27 to a controller based in Warsaw, for infringing Arts. 5(1)(f), 5(2), 25(1), 32(1) and (2) GDPR. This sanction was imposed in light of a data breach, which took place as a result of the exploitation of the controller's vulnerable IT system. Indeed, the SA held that the controller had infringed the principle of confidentiality as it did not put in place adequate safeguards, which would ensure that the data stored in its system is protected against unauthorised access.

Later in November, the Polish SA held that the processing of special categories of personal data of potential customers, as done by the controller Pionier, infringed Arts. 6(1), 5(1)(a) as well as 9(1) and (2) GDPR. Therefore, the controller was issued a fine of more than PLN 45,000 (approximately EUR 9,537) and ordered to cease processing the sensitive data without a legal basis.

6.2.1.20. PORTUGAL

On 11 February, the Portuguese SA concluded that the Portuguese National Statistics Institute had committed, in the context of processing data obtained from its national census survey, the following five GDPR violations:

- lack of lawfulness for the processing of special categories of personal data (Art. 9(1) GDPR);
- lack of compliance with transparency obligations (Arts. 12 and 13 GDPR);
- lack of a DPIA (Arts. 35(1), (2) and (3)(b) GDPR), including all the processing activities and relevant dimensions of Census;
- lack of due diligence concerning the choice of the processor (Arts. 28(1), (6) and (7) GDPR); and
- lack of compliance with the legal requirements for international data transfers (Arts. 44 and 46(2) GDPR), as interpreted by the Court of Justice of the European Union in the *Schrems II* ruling.

A single fine of EUR 4,300,000 was imposed on the controller.

In June, several telecom operators were ordered by the Portuguese SA to delete all the traffic and location data of its users. Such data had been stored for a year by the controllers in specific databases to help law enforcement authorities in their work of

investigating serious crimes. However, the SA argued that the processing of such data under Art. 4 of Law 32/2008 no longer enjoyed a legal basis and therefore, conflicted with the principle of lawfulness of Art. 5(1)(a) GDPR. Indeed, as a result of the Ruling 268/2022 in 2014, key provisions of Law 32/2008 (transposing the Data Retention Directive), such as Art. 4, were found unconstitutional.

6.2.1.21. ROMANIA

At the beginning of April, following an investigation of a personal data security breach consisting of the disclosure of the data of 32 employees, the Romanian SA sanctioned a controller with a corrective measure. It was discovered by the SA that the controller had infringed Art. 32(1)(b) and (2) GDPR, which led to the unauthorised disclosure through e-mail of a document containing the employees' personal data.

In May, the Romanian SA issued a fine of EUR 3,000 to the controller Wine Point SRL for violating Art. 32 GDPR by failing to take sufficient technical and organisational measures in order to ensure the confidentiality of the personal data processed. Indeed, the controller sent an e-mail to several individuals at the same time, thereby disclosing their e-mail addresses to everyone.

The same month, a courier company was sanctioned with a reprimand and a corrective measure by the Romanian SA. This sanction was issued as a result of the processor's breach of Art.32(1)(b), (2) and (4) GDPR.

In July, the cosmetic company Sephora Cosmetics Romania SA was sanctioned with a fine of EUR 2,000 for the breach of Art. 21 GDPR. The Romanian SA established that Sephora dismissed a request from the complainant not to use her personal data for marketing purposes. Indeed, after promising the complainant that her data would not be used, the controller still sent her unsolicited commercial messages.

In early September, the Romanian SA sanctioned a public institution for posting on its website 582 Excel files containing personal data of numerous individuals. It was established that the password for accessing the files had been disclosed, thereby increasing the risk of unauthorised access to the data. A reprimand, as well as a corrective measure, was issued by the SA on the institution for infringing Art. 32(1)(b) and (2) GDPR.

Later in September, the Romanian SA reprimanded the controller Târgu-Jiu Emergency County Hospital for infringing Art. 5(1)(a), (c) and (2) in conjunction with Art. 6 GDPR. The controller had published the complainant's personal data on the Internet without his consent and failed to answer the complainant's request. The complainant had asked to receive information regarding the personal data security policy as well as the reasons and the legal basis for disclosing his data. In addition to the fine, the SA ordered the controller to ensure that his processing operations complied with the GDPR and that the persons processing data under his authority be trained.

In October, a commercial company was sanctioned by the Romanian SA for collecting and disclosing on its website the personal data of natural persons and former employees of some companies without their consent. The controller was sanctioned with:

- a fine of EUR 5,000 for infringing Art.6(1) in conjunction with Art. 5(1)(a) GDPR;
- a reprimand for the breach of Art. 5(1)(d) GDPR; and
- a reprimand for the breach of Art. 14 corroborated with Art. 12 GDPR.

6.2.1.22. SLOVENIA

In 2022, the Slovenian SA handled several cases. A few cases of particular importance are presented in this section.

In July, the Slovenian police was ordered by the SA to reconsider a specific case as it did not determine all the substantial circumstances and facts. The case concerned an individual's request to access personal data (Art. 15 GDPR) regarding her entry in the Republic of Slovenia, through a particular border crossing point. The request was rejected by the controller for the reason that it did not keep a record of crossings at the national border. The complainant responded to the police's decision by filing an appeal.

In early October, the Slovenian SA ordered a controller to stop processing the location data of employees using its delivery vehicles. The SA found that the data was continuously, systematically and automatically processed by the controller through GPS tracking which enabled him to immediately determine who was using the company vehicle and where the employee was located. The SA concluded that the tracking was disproportionate to the aim pursued (i.e. safety of individuals in case of traffic incidents), there was no legal basis of legitimate interests for processing (Art. 6(1)(f) GDPR) and the GPS tracking infringed the principle of data minimisation (Art. 5(1)(c) GDPR).

Later in the month, an employer in the private sector was ordered by the Slovenian SA to remove its cameras monitoring work areas as it failed to fulfil the requirement of necessity. Indeed, the SA argued that other milder measures could have been used to monitor the compliance of work tasks (i.e. the use of machinery) with working safety rules, such as employees' statements or by using the data processed by the machinery itself.

In September, the Slovenian SA handled a case concerning a request made by an individual to receive the documents and information about the recipients of his data. In this case, the SA concluded that the documentation the complainant had asked to access, enclosed information about the market performance of an economic entity and not data of a natural person. Hence, the SA argued that there was no legal basis for the individual to receive the documents, nor the list of recipients of the data.

In December, a warning was issued by the Slovenian SA to a public penal institution for failing to put in place technical and organisational measures ensuring that video recordings would not be deleted. This warning was issued after an applicant had requested a copy of a video recording capturing his movements in a particular area of the prison during a specific date and was denied access to the data. It was established by the SA that the recording video had been automatically deleted by the controller after the request of the complainant had been submitted.

6.2.1.23. SPAIN

In 2021, the Spanish SA dealt with five cases involving the issuance of duplicate SIM cards to third parties other than subscribers. In those cases, the Spanish SA issued hefty fines for the violation of Art. 5(1)(f) GDPR. In separate decisions, the controllers Telefónica Móviles España, Orange Espagne, Xfera Móviles and Orange España Virtual were accused of failing to implement appropriate measures, thereby generating the loss of confidentiality and the transfer of personal data to a third party. The largest fine (EUR 3,940,000) was imposed on the controller Vodafone Espanã as not only did the company infringe Art. 5(1)(f) GDPR, but it also violated the principle of accountability under Art. 5(2) GDPR.

Furthermore, in March 2022, the Spanish SA imposed a fine of EUR 10,000,000 on the controller Google LLC for two infringements of the GDPR, namely lawfulness of processing (Art. 6) and the right to erasure (Art. 7). The Spanish SA found that the controller was transferring data without legitimacy to Lumen Database and was obstructing the right of erasure.

In 2022, the Spanish SA dealt with two cases concerning the processing of personal data on pornographic websites. The possibility that minors could register on the website and have direct,

uncontrolled access to pornographic content was a major problem in these cases. Upon registering, the minors' data was processed by the controllers. The Spanish SA ordered the controllers Burwebs S.L and Techpump Solutions S.L to implement, within a month, the necessary corrective measures to ensure that their activities complied with data protection regulations and that minors were effectively prevented from having access to the website's content. Additionally, the Spanish SA issued Burwebs a fine of EUR 75,000 for the infringement of Arts. 5(1)(a), (b) and (e), 8, 12(2), 13, 25 and 30 GDPR and Art. 22(2) of the Law of Information Society Services and Electronic Commerce (LSSI). On the other hand, Techpump Solutions was issued a fine of EUR 525,000 for the violations of Arts. 5(1)(a), (b) and (e), 6(1), 8, 12(1), 12(2), 13, 25 and 30 GDPR and Art. 22(2) LSSI.

6.2.1.24. SWEDEN

In this section, three enforcement measures conducted in 2022 by the Swedish SA for violations of the GDPR will be presented.

On 14 March, the Swedish Customs was issued an administrative fine of EUR 30,000 by the SA. It was established that the controller had not taken the necessary technical and organizational measures to prevent the data breach. Indeed, the technical barriers which had been set by the controller to restrict the storage and copying of data from staff mobiles in a US cloud service were not strong enough.

Later in the month, a financial company named Klarna was issued a fine of EUR 700,000 for numerous infringements of the GPDR. This includes the failure to provide information on the purpose and legal basis of the processing of personal data as well as to disclose to which non-EU countries the data was transferred to. Additionally, the Swedish SA discovered during its investigation that the controller has provided incomplete information about the data subject's rights.

The Swedish SA issued two separate fines in 2022 on different controllers within the same case, for breaching Art. 32 GDPR. In other words, both the Regional Board and the Hospital Board within the Region of Uppsala were condemned by the Swedish SA for failing to adequately secure the processing of sensitive data. The Regional Board was imposed an administrative sanction of EUR 30,000 as the information contained in the emails it had distributed to healthcare administrations within the region was not encrypted, thereby opening the door to unauthorised access. On the other hand, the Hospital Board was issued a fine of EUR 160,000, as not only did it fail to implement adequate security measures, but it also processed the data of patients in breach of Art. 5(1)(f) GDPR.

6.3. SA SURVEY - BUDGET AND STAFF

Statistics on resources made available by Member States to the SAs from the EEA are gathered by the EDPB each year. On 5 September 2022, the EDPB published an "Overview on resources made available by Member States to the Data Protection Supervisory Authorities". Most SAs (23) explicitly stated that their allocated budget is not sufficient for carrying out their activities, while some SAs considered they had sufficient financial resources. Based on information provided by 30 SAs from EEA countries prior to September 2022, five SAs saw budgetary decreases in contrast to their 2021 budget.

Eight SAs faced a decrease in employees compared to 2021. Overall, a vast majority of SAs (26) underlined that they do not have enough human resources to face their workload.

In its Contribution to the evaluation of the GDPR under Art. 97 adopted in 2020, the EDPB underlined that the SAs' ability to carry out their duties attributed by the GDPR is largely dependent on the resources made available to them.

7 COORDINATED SUPERVISION COMMITTEE OF THE LARGE EU INFORMATION SYSTEMS AND OF EU BODIES, OFFICES AND AGENCIES

As reflected in Art. 62 of Regulation 2018/1725, an active collaboration between the European Data Protection Supervisor (EDPS) and national Supervisory Authorities (SAs) is required to ensure the effective supervision of large-scale IT systems and of EU bodies, offices and agencies. While in the past the EDPS and the involved SAs cooperated through a system of individual Supervision Coordination Groups (SCGs),[55] in December 2019, the Coordinated Supervision Committee (CSC) was established within the EDPB to ensure the consistency of supervision efforts on all levels.

The CSC brings together the SAs of each EU Member State and the EDPS, as well as SAs of non-EU Members of the Schengen Area when foreseen under EU law. In the period between 2020-2022, the CSC carried out numerous notable tasks: it promoted and facilitated the exercise of data subject rights, examined the interpretation or application issues concerning EU and national law, exchanged relevant information, conducted joint audits and inspections, as well as prepared for the start of the activities of the European Public Prosecutor Office and other EU bodies and information systems falling under the Committee's scope.

Participation in the CSC meetings can occur under various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act.

Pursuant to Art. 62 of Regulation 2018/1725, the following EU large-scale IT systems, bodies, offices and agencies currently fall under the CSC's scope:

[55] In the past, four SCGs were created for the following systems: Schengen, Visa and Customs Information Systems, as well as for Eurodac.

Internal Market:

- Internal Market Information System (IMI), which allows the exchange of information between public authorities involved in the practical implementation of EU law.

Police and Judicial Cooperation:

- Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States;
- European Public Prosecutor Office (EPPO), the prosecution agency responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget;
- European Union Agency for Law Enforcement Cooperation (Europol).

In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the CSC, including:

Border, Asylum and Migration:

- Schengen Information System (SIS), ensuring border control cooperation;
- Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen States ;
- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen;
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States;
- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State;
- Customs Information System (CIS), which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation.

Police and Judicial Cooperation:

- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked ;
- Schengen Information System (SIS) (see above, as this system also fall under Police and Judicial cooperation).

More relevant info can be found in the EDPB's bi-annual report on the CSC.

8

ANNEXES

8.1. GENERAL GUIDANCE ADOPTED IN 2022

- Guidelines 01/2021 on Examples regarding Personal Data Breach Notification
- Guidelines 04/2021 on Codes of Conduct as tools for transfers (version 2.0)
- Guidelines 01/2022 on data subject rights - Right of access
- Guidelines 02/2022 on the application of Article 60 GDPR
- Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them
- Guidelines 04/2022 on the calculation of administrative fines under the GDPR
- Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement
- Guidelines 06/2022 on the practical implementation of amicable settlements
- Guidelines 07/2022 on certification as a tool for transfers
- Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority
- Guidelines 9/2022 on personal data breach notification under GDPR
- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)

8.2. CONSISTENCY OPINIONS AND DECISIONS ADOPTED IN 2022

- Decision 01/2022 on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR
- Binding Decision 2/2022 on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR
- Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)
- Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)
- Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR)
- Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria
- Opinion 02/2022 on the draft decision of the French Supervisory Authority regarding the

Controller Binding Corporate Rules of the WEBHELP Group

- Opinion 03/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the WEBHELP Group
- Opinion 04/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Norican Group
- Opinion 05/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Lundbeck Group
- Opinion 06/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Groupon International Limited
- Opinion 07/2022 on the draft decision of the Hungarian Supervisory Authority regarding the Controller Binding Corporate Rules of MOL Group
- Opinion 08/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Bioclinica Group
- Opinion 09/2022 on the draft decision of the Danish Supervisory Authority regarding the Processor Binding Corporate Rules of Bioclinica Group
- Opinion 10/2022 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Controller Binding Corporate Rules of Fresenius Group
- Opinion 11/2022 on the draft decision of the competent supervisory authority of Poland regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)
- Opinion 12/2022 on the draft decision of the competent supervisory authority of France regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)
- Opinion 13/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)
- Opinion 14/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR
- Opinion 15/2022 on the draft decision of the competent supervisory authority of Luxembourg regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR
- Opinion 16/2022 on the draft decision of the competent supervisory authority of Slovenia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR
- Opinion 17/2022 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the ANTOLIN Group
- Opinion 18/2022 on the draft decision of the Baden- Württemberg (Germany) Supervisory Authority regarding the Controller Binding Corporate Rules of the Daimler Truck Group
- Opinion 19/2022 on the draft decision of the Baden- Württemberg (Germany) Supervisory

Authority regarding the Controller Binding Corporate Rules of the Mercedes- Benz Group

- Opinion 20/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ellucian Group
- Opinion 21/2022 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Ellucian Group
- Opinion 22/2022 on the draft decision of the Liechtenstein Supervisory Authority regarding the Controller Binding Corporate Rules of Hilti Group
- Opinion 23/2022 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of the Samres Group
- Opinion 24/2022 on the draft decision of the Swedish Supervisory Authority regarding the Processor Binding Corporate Rules of the Samres Group
- Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors
- Opinion 26/2022 on the draft decision of the Data Protection Authority of Bavaria for the Private Sector regarding the Controller Binding Corporate Rules of the Munich Re Reinsurance Group
- Opinion 27/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of LEYTON Group
- Opinion 28/2022 on the Europrivacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR)
- Opinion 29/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the DSV Group
- Opinion 30/2022 on the draft decision of the Slovak Supervisory Authority regarding the Controller Binding Corporate Rules of Piano Group
- Opinion 31/2022 on the draft decision of the Slovak Supervisory Authority regarding the Processor Binding Corporate Rules of Piano Group
- Opinion 32/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ramboll Group

8.3. JOINT OPINIONS ADOPTED IN 2022

- EDPB-EDPS Joint Opinion 1/2022 on the extension of the Covid-19 certificate Regulation
- EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)
- EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space
- EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

8.4. LEGISLATIVE CONSULTATION

- Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework

- Statement 04/2022 on the design choices for a digital euro from the privacy and data protection perspective
- Statement on the implications of the CJEU judgment C-817/19 on the use of PNR in Member States
- EDPB Letter to the EU Commission on procedural aspects that could be harmonised at EU level
- Response of the EDPB to the European Commission's targeted consultation on a digital euro

8.5. OTHER DOCUMENTS

- Statement 02/2022 on personal data transfers to the Russian Federation
- Statement 03/2022 on the European Police Cooperation Code
- Statement on enforcement cooperation ('Vienna statement')
- EDPB Document on selection of cases of strategic importance

8.6. LIST OF EXPERT SUBGROUPS AND TASKFORCES WITH SCOPE OF MANDATES

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
Borders, Travel & Law Enforcement Expert Subgroup (BTLE)	• Law Enforcement Directive • Cross-border requests for e-evidence • Adequacy decisions under the Law Enforcement Directive, access to transferred data by law enforcement and national intelligence authorities in third countries • Passenger Name Records (PNR) • Border controls
Compliance, e-Government and Health Expert Subgroup (CEH)	• Codes of conduct, certification and accreditation • Compliance with public law and eGovernment • Processing of personal data concerning health • Processing of personal data for scientific research purposes • Consultation on several legislative proposals by the European Commission within the Digital Strategy • Close cooperation on DPIA with the Technology ESG focusing on the perspective of their mandates • Close cooperation on privacy by design and by default with the Technology ESG focusing on the perspective of their mandates
Cooperation Expert Subgroup (COOP)	• General focus on procedures of established by the GDPR for the purposes of the cooperation mechanism • Guidance on procedural questions linked to the cooperation mechanism • International mutual assistance and other cooperation tools to enforce the legislation for the protection of personal data outside the EU (Art. 50 GDPR)
Coordinators Expert Subgroup (COORD)	• General coordination between the Expert Subgroup Coordinators • Coordination on the annual Expert Subgroup working plan

Enforcement Expert Subgroup (ENF)	• Mapping/analysing the need for additional clarifications or guidance, based on practical experiences with the application of Chapters VI, VII and VIII GDPR • Mapping/analysing possible updates of existing Cooperation subgroup tools • Monitoring of investigation activities • Practical questions on investigations • Guidance on the practical application of Chapter VII GDPR including exchanges on concrete cases • Guidance on the application of Chapter VIII GDPR together with the Taskforce on Administrative Fines • Art. 65 and Art. 66 procedures
Financial Matters Expert Subgroup (FMESG)	Application of data protection principles in the financial sector (e.g. automatic exchange of personal data for tax purposes; impact of FATCA on the protection of personal data; interplay between Second Payment Services Directive and GDPR)
International Transfers Expert Subgroup (ITS)	Guidance on Chapter V (International transfer tools and policy issues), more specifically: • Review European Commission Adequacy decisions • Guidelines on Art. 46 GDPR and review of administrative arrangements between public authorities and bodies • Codes of conduct and certification as transfer tools • Art. 48 GDPR together with BTLE ESG • Art. 50 GDPR together with Cooperation ESG • Guidelines on territorial scope and the interplay with Chapter V of the GDPR – interaction with Key Provisions ESG • Exchange of information on review of BCRs and ad hoc contractual clauses according to Art. 64 GDPR

IT Users Expert Subgroup (IT-Users)	Developing and testing IT tools used by the EDPB with a practical focus: • Collecting feedback on the IT system from users • Adapting the systems and manuals • Discussing other business needs including tele- and videoconference systems
Key Provisions Expert Subgroup (KEYPROV)	Guidance on core concepts and principles of the GDPR, including Chapters I (e.g. scope, definitions like LSA and large-scale processing) and II (main principles); Chapters III (e.g. rights of individuals, transparency), IV (e.g. DPO – shared competences with CEH ESG, Enforcement ESG and Technology ESG) and IX
Social Media Expert Subgroup (SOCM)	• Analysing social media services, conceived as online platforms that focus on enabling the development of networks and communities of users, among which information and content is shared and whereby additional functions provided by social media services include targeting, personalisation, application integration, social plug-ins, user authentication, analytics and publishing • Analysing established and emerging functions offered by social media, including the underlying processing activities and corresponding risks for the rights and freedoms of individuals • Developing guidance, recommendations and best practices in relation to both the offer and use of social media functions, in particular for economic or political reasons • Providing assistance to other subgroups, in particular by proposing strategic priorities in terms of (a) supervision and (b) the development of new EDPB guidance or updating of existing WP29 guidance
Strategic Advisory Expert Subgroup (SAESG)	• Guidance on strategic questions affecting the whole EDPB (including the discussion on the strategy and on the work plans of the ESGs) • Clarification of questions that could not be resolved in the ESG
Taskforce on Administrative Fines (Fining-TF)	Development of Guidelines on the harmonisation of the calculation of fines

Technology Expert Subgroup (TECH)	• Technology, innovation, information security, confidentiality of communication in general • ePrivacy, encryption • DPIA and data breach notifications • Emerging technologies, innovation and other challenges related to privacy: reflecting on data protection risks of future technological developments • Providing input on technology matters relevant to other ESG

CONTACT DETAILS

Postal address
Rue Wiertz 60, B-1047 Brussels

Office address
Rue Montoyer 30, B-1000 Brussels

edpb
European Data Protection Board

An Executive Summary of this report, which provides an overview of key EDPB activities in 2022, is also available. Further details about the EDPB can be found on our website at edpb.europa.eu.