2021 ANNUAL REPORT

Enhancing the depth and breadth of data protection

edpb

European Data Protection Board

ENHANCING THE DEPTH AND BREADTH OF DATA PROTECTION

An Executive Summary of this report, which provides an overview of key EDPB activities in 2021, is also available.
Further details about the EDPB can be found on our website at edpb.europa.eu.

TABLE OF CONTENTS

1 GLOSSARY

Adequacy decision	An implementing act adopted by the European Commission that decides that a non-EU country ensures an adequate level of protection of personal data.
Binding Corporate Rules (BCRs)	Data protection policies adhered to by controller or processors established in the EU for transfers of personal data to controllers or processors outside the EU within a group of undertakings or enterprises or groups of enterprises engaged in a joint economic activity.
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 of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data that takes place in the context of the activities of a single establishment of a controller or processor in the Union, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
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 a data controller should limit the collection of personal data to what is directly adequate, relevant and limited to what is necessary to accomplish a specified purpose of the processing.

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)	A privacy-related impact assessment aiming to evaluate the processing of personal data, including notably its necessity and proportionality, an assessment of the risks for the rights and freedom of individuals, and the measures envisaged to address the risks.
Data Protection Officer (DPO)	An expert on data protection law and practices, 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 operations or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
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 or govern the relationship between controller and processor.
Supervisory Authority (SA)	An independent public supervisory body that monitors the application of the GDPR and other national laws relating to data protection, in order to protect the rights and freedoms of natural persons in relation to the processing of personal data. Also known as a Data Protection Authority (DPA).
Third country	A country outside the EU or EEA.

2 FOREWORD

2021 was the fourth year of existence and the first year of the multiannual EDPB Strategy 2021-2023. It was a very productive year, in which we completed many key actions to reach the objectives set out in our Strategy.

Though we continued to work mostly remotely due to the continuing impact of the COVID-19 pandemic, we made significant progress on a number of important files. To make this possible, we held over 380 EDPB meetings. Here, I outline some highlights from our work over the past year.

Firstly, the EDPB continued to pay a great deal of attention to international transfers of personal data. In 2021, we adopted the final version of our Recommendations on supplementary measures following the *Schrems II* ruling by the Court of Justice of the EU, taking on board the input received from stakeholders during public consultation. These recommendations lay out a clear roadmap of steps data exporters can follow to identify and implement appropriate supplementary measures to ensure an essentially equivalent level of protection for the personal data they transfer to third countries.

The EDPB also adopted Opinions on the UK draft adequacy decisions. While adequacy findings are available to those countries that meet the relevant criteria, EU data protection legislation offers other transfer mechanisms. In line with this, we adopted Guidelines on codes of conduct as tools for transfers. In addition, we issued a Joint Opinion together with the EDPS on a new set of Standard Contractual Clauses (SCCs) issued by the European Commission for the transfer of personal data to controllers and processors established outside the EEA. We worked closely together with the European Commission to ensure full consistency between the SCCs and our Recommendations on supplementary measures.

A second area in which we carried out important work in 2021 was digital policy. In the framework of the EU's Digital Strategy, the European Commission put forward several proposals on which the EDPB, together with the European Data Protection Supervisor (EDPS), issued legislative advice. The EDPB and EDPS adopted a Joint Opinion on the proposal for a Data Governance Act (DGA) and a statement on the Digital Service Package and Data Strategy. We also adopted an important Joint Opinion with the EDPS on the draft Artificial Intelligence Act. It is crucial that the future DGA and data processing acts under the Artificial Intelligence Act are fully in line with EU personal data protection legislation.

Law enforcement was a third priority area that underscored our work in 2021. Adequacy decisions may also be adopted in the framework of the Law Enforcement Directive (LED). Last year, we adopted recommendations on the LED adequacy referential. By detailing the core data protection principles that have to be present in the third country legal framework to ensure essential equivalence with the EU framework, our guidance aims to standardise the adequacy procedure under the LED. We also carried out an evaluation of the LED itself.

Throughout 2021, we issued several guidance documents to clarify the terms of European data protection law for companies and organisations. For example, we published examples of data breach notifications and guidance on virtual voice assistants. We also adopted the final version of our Guidelines on the concepts of controller and processor and Guidelines on the targeting of social media users, after incorporating stakeholders' feedback. By interacting and consulting with stakeholders, we aim to make our guidance practical and concrete, answering the needs identified by our stakeholders.

Naturally, a topic that is high on our priority list is the enforcement of the GDPR. So far, the national Supervisory Authorities have worked or are working together on almost 2,000 cross-border cases. The dispute resolution mechanism under Art. 65 GDPR has been triggered twice (once in 2020 and once in 2021) and, in 2021, we also dealt with our first Art. 66 GDPR urgency procedure relating to national provisional measures imposed in Germany against WhatsApp data-sharing practices with Facebook.

In the coming year we will continue to develop guidance to help stakeholders understand and interpret the GDPR. We have set out ambitious goals for 2022, including work on guidance on topics as varied as legitimate interest as a legal basis and the use of facial recognition by law enforcement authorities.

In 2022, we will also continue our work to optimise cooperation and enforcement. A dedicated meeting at the level of the heads of the Supervisory Authorities (SAs) will allow them to share experiences and discuss practical ways to ensure effective and efficient cooperation among SAs.

We see our internal discussions against the backdrop of a broader international debate on cooperation and we aim to invest further resources in the global dimension of data protection. We make a continuous effort to meet and exchange good practices with our colleagues worldwide, through fora such as the Global Privacy Assembly and the G7.

Undoubtedly, the depth and breadth of our work is all thanks to the efforts of everyone within the EDPB, accompanied by the valuable collaborative input and engagement of all stakeholders in our consultations and events.

Andrea Jelinek

Chair of the European Data Protection Board

3

2021 - HIGHLIGHTS

3.1. STRATEGY 2021-2023 AND WORK PROGRAMME 2021-2022

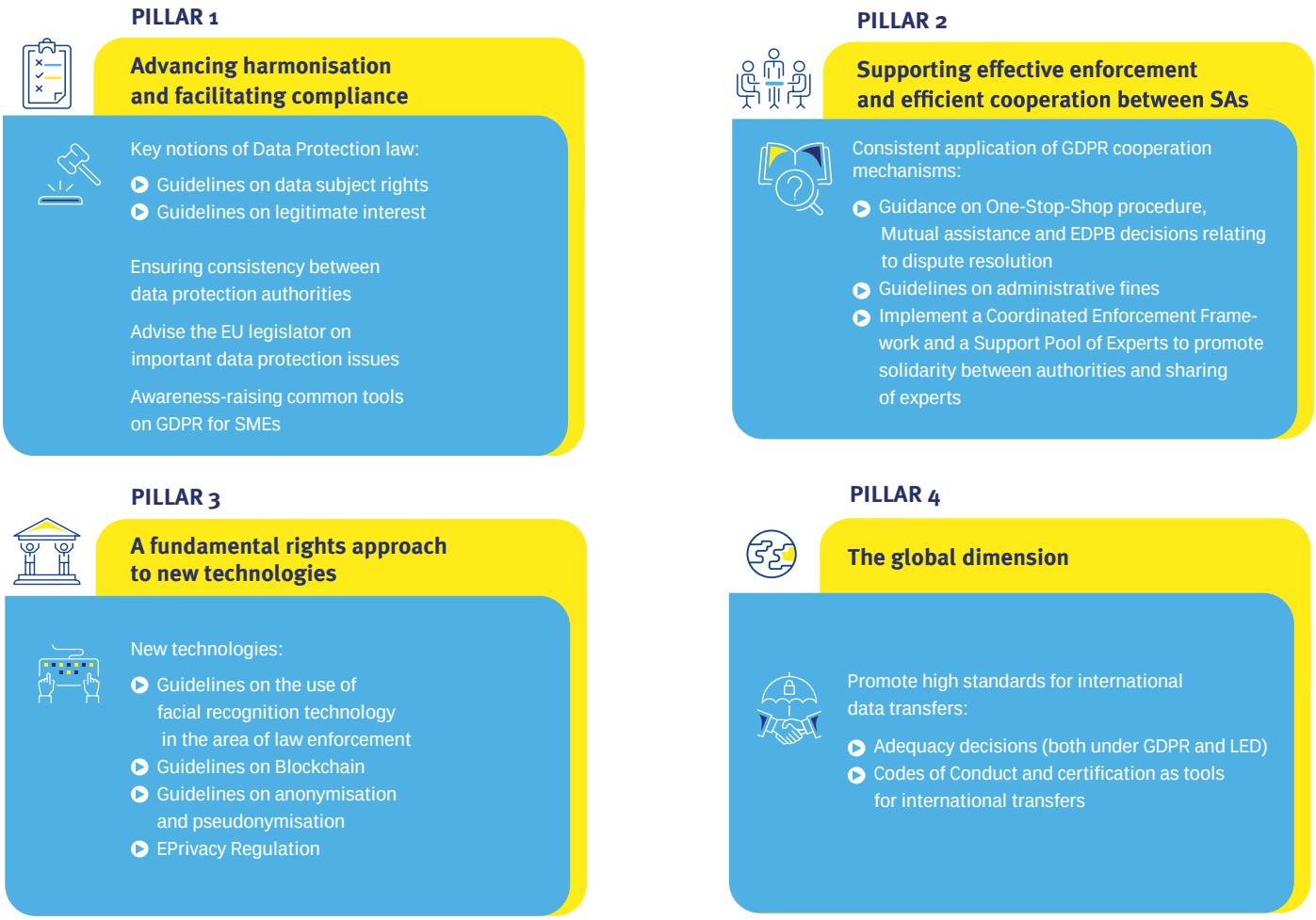
In early 2021, the EDPB adopted its two-year Work Programme for 2021-2022, according to Art. 29 of the EDPB Rules of Procedure. The work programme follows the priorities set out in the Strategy for 2021-2023 and will put these into practice.

This Strategy includes four main pillars, as well as a set of three key actions per pillar to help achieve these goals. The pillars and key actions are illustrated below.

The EDPB Strategy and Work Programme will help guide the EDPB's work in 2021 and the years to come. The tools included in the Work Programme will help create a more consistent understanding of the key concepts and processes in the GDPR and the cooperation and consistency mechanism in particular. This will allow the EDPB to reinforce its leadership in ensuring consistency across the EEA and further drive EEA SAs to work in one direction and to speak in one voice.

3.2. EDPB OPINIONS ON DRAFT UK ADEQUACY DECISIONS

The EDPB issued two opinions on the European Commission draft Implementing Decisions on the adequate protection of personal data in the UK. Opinion 14/2021 is based on the GDPR and assesses both general data protection aspects and government access to personal data transferred from the EEA for the purposes of law enforcement and national security included in the draft adequacy decision. Opinion 15/2021 is



based on the Law Enforcement Directive (LED) and analyses the draft adequacy decision in the light of Recommendations 01/2021 on the adequacy referential under the LED (see Section 5.1.2 of this Report), as well as the relevant case law reflected in Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. This is the first draft implementing decision on a third country's adequacy under the LED ever presented by the European Commission and assessed by the EDPB.

3.2.1. Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive

The EDPB issued recommendations to provide guidance to the European Commission on the level of data protection in third countries and international organisations under the LED. The finding of an adequate level of data protection does not need to demonstrate a point-by-point mirroring of EU legislation, but rather that the core requirements of legislation in a third country are effective (i.e. enforced and followed in practice) in ensuring a level of protection in the third country essentially equivalent to that guaranteed in the EU.

To be able to properly advise the European Commission pursuant to Art. 51(1)(g) LED on adequacy decisions, the EDPB should receive all relevant documentation, including relevant correspondence and the findings made by the European Commission, so it can assess the European Commission's analysis. The EDPB should also be kept informed of periodic reviews of adequacy decisions under Art. 36(5) LED and of any action by the European Commission to repeal, amend or suspend adequacy decisions.

As part of an assessment of the level of data protection offered by a third country or international organisation, consideration should be given to:

- The consistency of general principles and safeguards with EU data protection law;
- Principles applied to the processing of special categories of data, automated decision making and profiling, and the application of the principles of data protection by design and default;
- Procedural and enforcement mechanisms in the third country or international organisation;
- Whether the guarantees set out in the EDPB's Recommendations 02/2020 have been taken into account in the third country or international organisation when assessing the adequacy of a third country under the LED in the field of surveillance.

Adopted: 2 February 2021

3.2.2. Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom

When providing an assessment of the draft implementing decision on the adequacy of personal data protection offered by the UK under the GDPR, the EDPB finds that many aspects of the UK's data protection framework are essentially equivalent to those in the EU. The EDPB welcomes the UK's continued adherence to the European Convention on Human Rights and Council of Europe Convention 108, and current work on ratifying Convention 108+.

However, there are several potential challenges to seeing the UK's data protection framework as essentially equivalent to that of the EU, including:

- Future possible divergences between UK legal framework and EU data protection law, which require close monitoring by the European Commission;
- The broad formulation of an "immigration exemption" to the application of data subject rights;
- The risk of onward transfer from the UK of personal data received from the EEA to third countries that might undermine the level of protection of the personal data if the rules applicable in the UK to onward transfers do not ensure that an essentially equivalent level of protection will continue to be provided;
- The potential impact of international agreements facilitating access to personal data in the UK by public authorities in third countries.

Due to the potential for the UK to diverge from EU data protection law, the EDPB welcomes the inclusion of a sunset clause, and invites the Commission to monitor closely all relevant developments in the UK that may have an impact on

the essential equivalence of the level of protection of personal data and, where necessary, to take swiftly appropriate actions, such as suspending, amending or repealing the adequacy decision.

Adopted: 13 April 2021

3.2.3. Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom

In considering the Commission's draft decision on the adequacy of personal data protection under the LED, the EDPB recognises that many aspects of its data protection framework are essentially equivalent to the protections offered in the EU. The EDPB welcomes the UK's continued adherence to the European Convention on Human Rights and Council of Europe Convention 108, and current work on ratifying Convention 108+.

Noting the possibility that the UK deviates in the future from the EU data protection framework, the EDPB welcomes the addition of a sunset clause into the draft decision. The EDPB highlights the importance of the Commission closely monitoring developments in the UK's data protection framework such as international agreements between the UK and third countries or adequacy decisions adopted by the UK based on standards diverging from the EU's that may undermine the essentially equivalent level of protection of personal data transferred from the EU. Should there be developments entailing that an adequate level of protection can no longer be ensured in the UK, the EDPB recommends to the Commission that the adequacy decision is suspended, amended or repealed, as appropriate.

Adopted: 13 April 2021

3.3. FURTHER GUIDANCE AND OPINIONS FOLLOWING THE CASE C-311/18 *SCHREMS II* RULING BY THE CJEU

3.3.1. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – Version 2.0

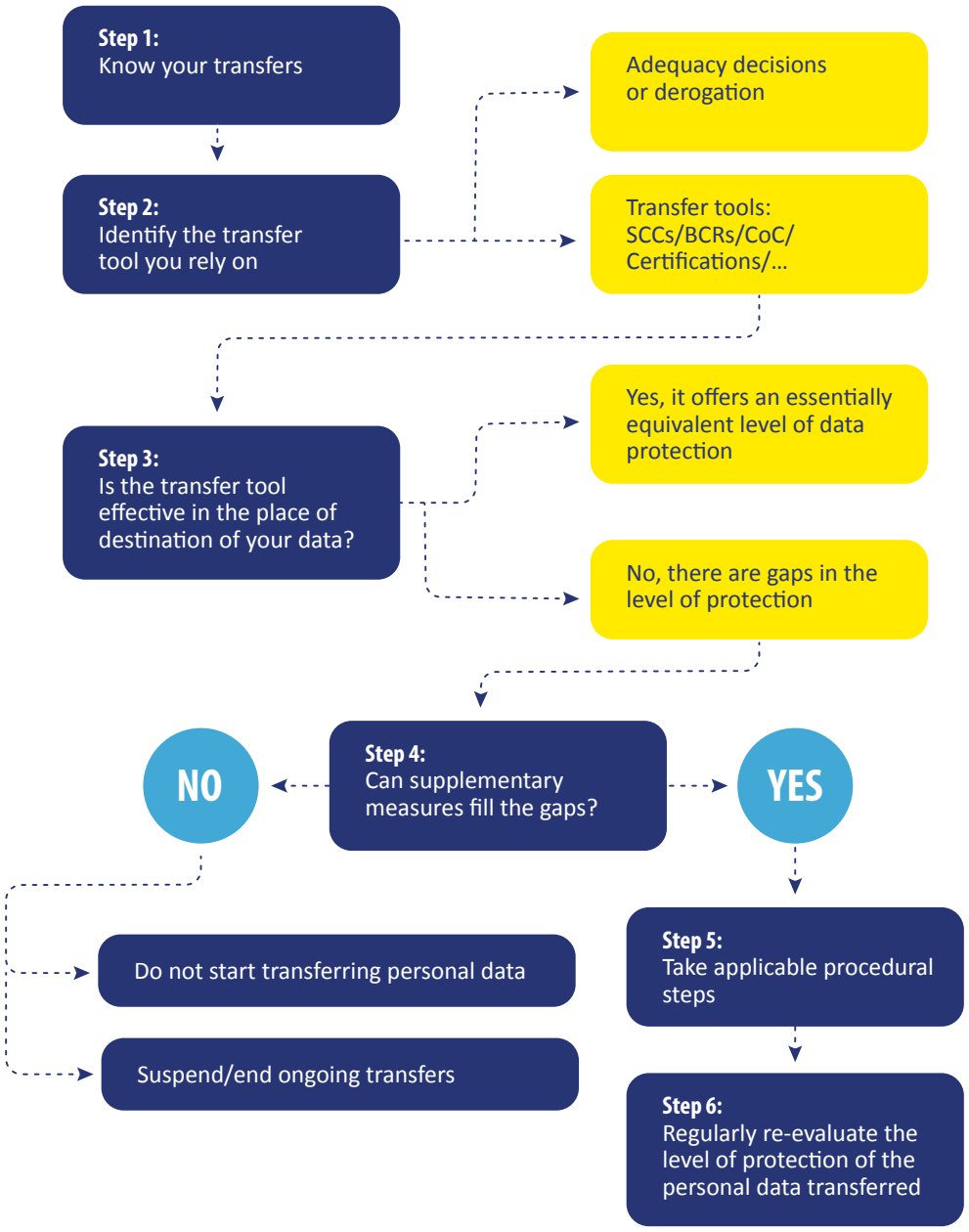
As part of its guidance work following the Case C-311/18 *Schrems II* ruling by the CJEU, the EDPB adopted a final version of its Recommendations 01/2020 following the public consultation that took place at the end of 2020. These aim to help exporters (including controllers, processors, private entities and public bodies) with the complex task of assessing third countries and identifying appropriate supplementary measures where they are needed. Data exporters may need to adopt supplementary measures to ensure that the data they transfer to specific third countries is afforded a level of protection essentially equivalent to that guaranteed in the EU. These recommendations provide data exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place. The recommendations complement and are consistent with the final version of the European Commission's Standard Contractual Clauses (SCCs) for international data transfers. The EDPB and the European Commission worked together to achieve this. These steps are illustrated below.

3.3.2. EDPS-EDPB Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries

The EDPB and EDPS adopted Joint Opinion 02/2021 on SCCs developed by the European Commission in accordance with Art. 46(1)(c) GDPR relating to the transfer of personal data to third countries. The draft SCCs update and replace the existing

Roadmap: applying the principle of accountability to data transfers in practice

Roadmap: applying the principle of accountability to data transfers in practice



SCCs for international transfers that were adopted on the basis of Directive 95/46, and take account of the new requirements under the GDPR and the *Schrems II* judgement of the CJEU. Joint Opinion 02/2021 makes clear that the recommendations on supplementary measures are complementary to the SCCs and should therefore guide exporters on how to apply the SCCs correctly. The EDPB also adopted Joint Opinion 01/2021 on standard contractual clauses between controllers and processors under Art. 28(7) GDPR (see Section 5.5.5 for a full summary).

Adopted: 18 June 2021

3.4. EDPB-EDPS JOINT OPINION 05/2021 ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT)

The European Commission presented its Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) on 21 April 2021. AI technologies often involve processing of personal data, so the proposal has important data protection implications. The EDPB and the EDPS adopted Joint Opinion 5/2021. The EDPB and the EDPS raise the following issues:

- **Scope.** The proposal's scope should be expanded so it includes international law enforcement cooperation. Also, it should be clarified in the main text of the proposal that the EU data protection legislation applies to any processing of personal data falling within the scope of the proposal;
- **Risk-based approach and alignment with the GDPR.** The proposal should be aligned with the GDPR when it comes to the concept of "risk to fundamental rights", as well as regarding the rights and remedies available to individuals;
- **Prohibited uses of AI.** Considering high-risk of intrusion into individuals' private lives, great risk of discrimination and effect on human dignity, certain use of AI should be prohibited. In particular, the future regulation should include a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces and should prohibit any type of social scoring. It is also recommended to ban AI systems that categorize individuals from biometrics into clusters, as well as those that infer emotion of natural persons;
- **High-risk AI systems.** External third parties should conduct ex-ante conformity assessments;
- **Governance and European AI Board.** The tasks of the EDPS as the competent authority and the market surveillance authority for the supervision of the Union institutions, agencies and bodies need to be clarified. Data protection authorities should be designated as national supervisory authorities for AI systems considering their expertise and the proposal's close link with the data protection framework. The supervisory authorities for AI systems must be completely independent in the performance of their task in order to guarantee proper supervision and enforcement. The European AI Board (EAIB) should be given more autonomy and powers, moreover, it's legal status should be clarified;
- **Regulatory sandboxes and interaction with the data protection framework.** The concept of regulatory sandboxes should be specified, and the EAIB should provide common guidelines on their use. Clarification is needed on compliance mechanisms, particularly on their scope and relationship with other existing measures, such as data protection certifications, seals, marks and codes of conduct.

Adopted: 18 June 2021

3.5. BINDING DECISION 01/2021 ON THE DISPUTE ARISEN ON THE DRAFT DECISION OF THE IRISH SUPERVISORY AUTHORITY REGARDING WHATSAPP IRELAND UNDER ART. 65(1)(A) GDPR

The EDPB adopted a binding decision based on Art. 65(1)(a) GDPR which sought to address the lack of consensus on certain aspects of a draft decision issued by the Irish SA as lead supervisory authority (LSA) regarding WhatsApp Ireland Ltd. (WhatsApp IE) and the subsequent objections expressed by a number of concerned supervisory authorities (CSAs). The Irish SA issued the draft decision following an own-volition inquiry into WhatsApp IE, concerning whether WhatsApp IE complied with its transparency obligations pursuant to Arts. 12, 13 and 14 GDPR.

When the Lead Supervisory Authority (LSA) submits a draft decision to the Concerned Supervisory Authorities (CSAs), they may then raise "relevant and reasoned objections" within the set timeframe. Art. 65(1)(a) GDPR requires the EDPB to issue a binding decision when the LSA decides not to follow a relevant and reasoned objection expressed by a CSA or is of the opinion that the objection is not relevant or reasoned. The EDPB sought to clarify the key concepts of this mechanism via two sets of guidelines. First, Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 were adopted in 2020 and finalised after public consultation in March 2021. Second, Guidelines 03/2021 specifically focused on the application of Art. 65(1)(a) GDPR and were adopted in 2021.

In this decision, which was the second instance of application of Art. 65(1)(a) GDPR, after the binding decision adopted in 2020 addressing a dispute concerning the Irish SA's draft decision on Twitter International Company, the EDPB concluded that the Irish SA should amend its draft decision on WhatsApp IE regarding infringements of transparency, the period to bring processing operations into compliance and the calculation of the fine.

The EDPB analysed the merits of the objections it found to meet the "relevant and reasoned" threshold set by Art. 4(24) GDPR and requested the Irish SA introduce some amendments in its draft decision.

Regarding transparency, the draft decision by the Irish SA already identified a severe breach of Arts. 12 to 14 GDPR. The EDPB identified additional shortcomings with the information provided, affecting users' ability to understand the legitimate interests being pursued. Therefore, the EDPB requested that the Irish SA to include a finding of an infringement of Art. 13(1)(d) GDPR in its decision. The binding decision also included a request to include a formal finding of an infringement of Art. 13(2)(e) GDPR.

In addition, the EDPB clarified that, while not every infringement of Arts. 12 to 14 GDPR necessarily entails an infringement of Art. 5(1)(a) GDPR, in this particular case, in light of the gravity and the overarching nature and impact of the infringements, there has been an infringement of the transparency principle enshrined in Art. 5(1)(a) GDPR.

Regarding WhatsApp IE's collection of data of non-users when users decide to use the Contact Feature functionality, the EDPB found that the procedure used by WhatsApp IE did not lead to anonymisation of the collected personal data. Therefore, the EDPB also found that the infringement of Art. 14 GDPR extended to WhatsApp IE's processing of non-users' personal data.

Regarding the imposed fine and the calculation of the fine, the EDPB decided that the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Art. 83(4)-(6) GDPR, but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Art. 83(1) GDPR. In this case, the EDPB found the consolidated turnover of the parent company (Facebook Inc.) was to be included in the turnover calculation.

In addition, the EDPB clarified its interpretation of how the calculation of the fine was influenced by the finding of several infringements under Art. 83(3) GDPR. When faced with multiple infringements for the same or linked processing operations, all the infringements should be taken into consideration when calculating the amount of the fine. This is notwithstanding the duty on SAs to take into account the proportionality of the fine and to respect the maximum fine amount set out by the GDPR.

The EDPB also analysed the criteria set by Art. 83(1) and (2) GDPR and concluded that the proposed fine did not adequately reflect the seriousness and severity of the infringements nor did it have a dissuasive effect. Hence, the EDPB instructed the Irish SA to reassess its envisaged fine in accordance with the conclusions reached and impose a higher fine amount.

The Irish SA draft decision included an order to WhatsApp to bring processing operations into compliance within a period of six months. The EDPB found it of primary importance that compliance with transparency obligations was ensured in the shortest timeframe possible. As such, the Irish SA was requested to amend the six-month deadline for compliance to a period of three months.

Adopted: 28 July 2021

3.6. URGENT BINDING DECISION 01/2021 ON THE REQUEST UNDER ART. 66(2) GDPR FROM THE HAMBURG (GERMAN) SUPERVISORY AUTHORITY FOR ORDERING THE ADOPTION OF FINAL MEASURES REGARDING FACEBOOK IRELAND LIMITED

The EDPB adopted its first urgent binding decision under Art. 66(2) GDPR following a request from the Hamburg SA, which had adopted provisional measures against Facebook Ireland Ltd. (Facebook IE) under Art. 66(1) GDPR. The provisional measures prohibited Facebook IE from processing, for 3 months, the data of German residents using WhatsApp for Facebook IE's own purposes, following a change in the Terms of Service and Privacy Policy applicable to European users of WhatsApp IE.

The EDPB decided that the conditions to prove the existence of an infringement to the GDPR and the urgency to adopt final measures were not met, hence stating that the Irish SA did not need to adopt final measures against Facebook IE.

On the issue of an infringement, the EDPB concluded there was a high likelihood that Facebook IE was already processing WhatsApp's user data as a (joint) controller for the common purposes of (i) safety, security and integrity of WhatsApp IE and the other Facebook Companies,[1] and of (ii) improvement of the products of the Facebook Companies. However, due to various contradictions, ambiguities and uncertainties in WhatsApp's user-facing information and written commitments by Facebook IE and WhatsApp IE, the EDPB decided that it was not able to determine with certainty which processing operations are actually being carried out and in which capacity.

Moreover, the EDPB did not have enough information to determine with certainty whether Facebook IE had already started to process WhatsApp's user data as a (joint) controller for its own purposes of marketing communications and

direct marketing, and cooperation with the other Facebook Companies. The EDPB could also not conclude whether Facebook IE had already started or would soon start processing WhatsApp's user data as a (joint) controller for its own purpose in relation to WhatsApp Business API.

On the existence of urgency, the EDPB rejected the Hamburg SA's argument based on Art. 61(8) GDPR as it did not demonstrate that the Irish SA had failed to provide information in the context of a formal request for mutual assistance under Art. 61 GDPR. Besides, the EDPB decided that the adoption of WhatsApp IE's Updated Terms, which contained similar problematic elements as the previous terms, could not, on its own, justify the urgency for the EDPB to order the Irish SA to adopt final measures. Consequently, the EDPB concluded that there was no urgency for the Irish SA to issue final measures against Facebook IE in this case.

However, considering the high likelihood of infringements in particular for the purposes of (i) safety, security and integrity of WhatsApp IE and the other Facebook Companies, and of (ii) improvement of the products of the Facebook Companies, the EDPB requested the Irish SA to perform, as a matter of priority, a statutory investigation. In particular, to show whether Facebook IE was processing WhatsApp user data for such a common purpose of Facebook Companies as a (joint) controller. The Irish SA was requested to verify whether, in practice, Facebook Companies were carrying out processing operations, which implies the combination or comparison of WhatsApp IE's user data with other data sets processed by other Facebook Companies in the context of other apps or services offered by the Facebook Companies, facilitated *inter alia* by the use of unique identifiers. The EDPB asked the Irish SA to determine whether such processing activities were taking place or not and, if they were, whether they had a proper legal basis under Art. 5(1)(a) and Art. 6(1) GDPR.

In addition, taking into consideration the lack of information as regards how personal data are processed for marketing purposes, cooperation with other Facebook Companies and in relation to WhatsApp Business API, the EDPB called upon the Irish SA to further investigate the role of Facebook IE, i.e. whether Facebook IE was acting as a processor or a (joint) controller, with respect to these processing operations.

Adopted: 12 July 2021

[1] "Facebook Companies" refers to the term as it was defined by WhatsApp in its public-facing information at the time when the EDPB adopted its urgent binding decision (i.e. before the Facebook Group was renamed Meta Group).

4

2021 - THE EDPB SECRETARIAT

4.1. THE EDPB SECRETARIAT

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

A Memorandum of Understanding establishes the terms of cooperation between the EDPB and the EDPS. The staff at the EDPB Secretariat are employed by the EDPS, however, they only work under the instructions of the Chair of the EDPB. At the end of 2021, the staff of the EDPB Secretariat was composed of 31 FTE staff members: one head of the EDPB Secretariat, 6 heads of activity, 12 legal officers, 4 communication officers, 6 administrative assistants and 2 IT officers. The EDPB Secretariat also received the support of three IT external contractors.

The EDPB Secretariat led the drafting of over 35% of the guidelines, opinions, recommendations and statements adopted by the EDPB in 2021 and contributed to a further 25%. In particular, the EDPB Secretariat led the drafting of the Recommendation 01/2020 on the supplementary measures; the EDPB binding decisions (under Art. 65 and Art. 66 GDPR), and the EDPB Strategy and Work Programme.

The EDPB held 389 meetings, including 15 plenary meetings, 200 expert subgroup meetings and 174 drafting team meetings, in comparison to about 100 meetings per year held before the pandemic.

4.2. THE EDPB SECRETARIAT'S CONTRIBUTION TO THE NATIONAL SAs' COOPERATION

As part of its 2021-2023 Strategy, the EDPB established a Support Pool of Experts (SPE) in 2020. The terms of reference of the SPE specify that its objectives are to provide material support to the EDPB Members in the form of expertise that is useful for investigations and enforcement activities, and to enhance cooperation and solidarity between the EDPB Members by sharing, reinforcing and complementing strengths and addressing operational needs. In October 2021, a new Head of Activity for Enforcement Support and Coordination was appointed to coordinate the work of the SPE and, in December 2021, EDPB members agreed on SPE priorities for 2022.

Further in line with the 2021-2023 Strategy, the EDPB set up a Coordinated Enforcement Framework (CEF). The CEF provides a structure for recurring annual coordinated action by the SAs. The CEF aims to facilitate joint actions in a flexible and coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations. The purpose behind the recurring annual coordinated actions is to promote compliance, empower data subjects to exercise their rights and raise awareness. EDPB members agreed to launch the first coordinated action in 2022 on the use of Cloud based services by the public sector. The EDPB Secretariat is contributing to this work.

The EDPB Secretariat is also in charge of the management of a register on the EDPB website gathering the final decisions taken concerning cross-border cases in the context of the One-Stop-Shop (OSS) mechanism. The register offers an exceptional opportunity to read final decisions taken by, and involving, different SAs in a cross-border context. These decisions often contain useful guidance on how to comply with the GDPR in practice. The register contains both final decisions and summaries prepared by the EDPB Secretariat and duly approved by LSAs. See more information under Section 6.1.3 of this Annual Report.

In the context of cooperation between SAs in the assessment of Binding Corporate Rules (BCR) applications, the EDPB Secretariat organised four BCR sessions in 2021. The sessions streamlined discussions between the SAs and the EDPB Secretariat regarding specific aspects of individual BCRs with the aim to facilitate the assessment of the BCRs and work out a consensus on the standards and expectations for BCRs, before the formal procedure is triggered under Art. 64 GDPR. The BCR sessions thus represent a prior informal cooperation phase that aims to address remaining issues that have arisen regarding a specific BCR based on shared comments by the SAs and the EDPB Secretariat.

Additionally, several informal sessions were organised regarding certification criteria. These sessions fostered discussion between the SAs and the EDPB Secretariat on specific certification criteria that may be submitted to the EDPB under Art. 64(1)(c) GDPR.

4.3. IT COMMUNICATIONS TOOL (INTERNAL MARKET INFORMATION) AND THE NEW EDPB WEBSITE

With regard to the technical support for SAs' cooperation, throughout 2021, the EDPB Secretariat continued to provide support to the SAs with IT solutions that facilitate their communication. In this respect, the EDPB Secretariat leads the IT Users Expert Subgroup which focuses on assessing the need for development and making changes to the IMI system. Furthermore, it continued to work on best practices to further refine the procedures in use and to share its expertise on the use of the IMI System for the cooperation and consistency mechanism. The EDPB Secretariat also provides an IMI helpdesk to support the staff of the SAs making use of the IMI system. The EDPB IMI helpdesk dealt with 331 requests for support from SAs, and carried out 159 proactive monitoring

procedures to ensure that case files were complete and correctly registered.

The EDPB Secretariat also migrated the EDPB Wiki platform used for internal sharing of information to a new instance dedicated to the EDPB and with an enhanced user experience.

In 2021, the EDPB Secretariat enhanced the EDPB website, 'edpb.europa.eu', which underwent a new web design.

In the context of functionality, the website now supports dynamic listing of documents and filters, which improves user experience by eliminating numerous general search queries. The communication functionality was improved by providing a new contact form on the website. The content management system of the website, which manages the creation and modification of digital content, was upgraded to Drupal 8. The EDPB Secretariat is also putting great efforts into implementing a new advanced search functionality that will make the website more user-friendly.

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

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

In 2021, the EDPB received 39 public access requests for documents held by the EDPB. Confirmatory applications were received in two cases. The EDPB Secretariat is in charge of preparing the answers to those requests, subject to the validation of the EDPB Chair (for confirmatory applications) and Deputy chairs (for initial applications), in accordance with Art. 32(2) of the EDPB Rules of Procedure.

A complaint was made to the European Ombudsman regarding an EDPB confirmatory decision for a request for access to documents, which was submitted in 2020.[2] The request concerned access to some of the preparatory documents for the EDPB Guidelines 02/2019 on the processing of personal data in the context of the provision of online services to data subjects. Following a reassessment of the documents, the EDPB decided to grant partial access to these documents as the fact that differing views expressed in the documents were already publicly known. The complainant was satisfied with the EDPB's reply and the Ombudsman decided to close the case.

[2] Decision on the EDPB's refusal to grant public access to the preparatory documents for its Guidelines on the processing of personal data in the context of the provision of online services (case 86/2021/AMF).

4.5. THE EDPB SECRETARIAT'S ACTIVITIES RELATING TO DATA PROTECTION OFFICER ACTIVITIES

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

In 2021, the EDPB, with the assistance of its DPO team, continued to strengthen the compliance with Regulation 2018/1725 by enhancing its transparency practices through different means, such as:

- The development, publication and update of several privacy notices;
- The continued development of several records, as well as a centralised register for records, which will be made available on the EDPB website;
- The update of its DPO website page with additional information; and
- The improvement of its contact form on the EDPB website.

Furthermore, the DPO team launched several internal legal assessments on various issues concerning the EDPB's processing of personal data and identified suitable legal, organisational and, where applicable, technical solutions. The assessments were also conducted as part of the DPO's advisory role for the EDPB.

In 2021, the DPO team assisted with the handling of six data subject requests under Art. 17 to Art. 24 of Regulation 2018/1725, which indicates a decrease in relation to 2020.

Regarding data breaches, the DPO team assisted with the handling of 12 data breaches under Arts. 34 and 35 of Regulation 2018/1725, which represents an increase in relation to 2020. The assessment of the majority of these data breaches indicated that they were unlikely to result in a risk to the rights and freedoms of natural persons. At the time of the drafting of this report, only one data breach had required a notification to the EDPS.

The DPO team also assisted with several replies to individual requests for information involving the processing of their personal data, including cases where individuals mistakenly assumed that the EDPB processed their personal data.

In addition, the DPO team delivered several internal training sessions and created awareness-raising material, aimed at EDPB Secretariat staff. These activities were tailored to the needs and expertise of the participants to ensure that all staff members, in particular newcomers, were adequately informed of their duties regarding personal data processing, but also of their rights as data subjects.

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

5

EUROPEAN DATA PROTECTION BOARD - ACTIVITIES IN 2021

To ensure the consistent application of the GDPR across the EEA, the EDPB issues general guidance to clarify European data protection laws. This guidance provides the public and stakeholders with a consistent interpretation of their rights and obligations, and ensures that national Supervisory Authorities (SAs) have a benchmark for applying and enforcing the GDPR. The EDPB is also empowered to issue opinions or binding decisions to guarantee the consistent application of the GDPR by SAs. Throughout 2021, the EDPB issued multiple guidance and consistency documents, as summarised below.

5.1. GENERAL GUIDANCE (GUIDELINES AND RECOMMENDATIONS)

In 2021, the EDPB adopted several guidelines and recommendations on the data protection requirements pertaining to data breach notifications, on codes of conduct as data transfer tools, storing credit card data, virtual voice assistants and the meaning of specific terms in the GDPR. These guidelines and recommendations are summarised below.

5.1.1. Guidelines 01/2021 on examples regarding personal data breach notification

The EDPB guidelines aim to help data controllers in deciding how to handle personal data breaches and what factors to consider during risk assessment. Art. 4(12) GDPR defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". The practice-oriented, case-based guidance complements the Article 29 Working Party Guidelines on personal data breach notification under Regulation 2016/679, WP 250 and reflects the common experiences of the EEA SAs since the GDPR became applicable.

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

1. **Ransomware attacks** involve malicious code encrypting personal data, where the attacker requires a ransom in exchange for a decryption code.
2. **Data exfiltration attacks** exploit vulnerabilities in services offered over the internet and usually aim to copy, exfiltrate and abuse personal data for some malicious end.
3. **Internal human-related risk source** refers to human errors that lead to personal data breaches, which can have a frequent occurrence and can be both deliberate and accidental, therefore making it difficult for data controllers to identify weaknesses and take steps to avoid them.
4. **Loss or theft of devices and/or documents** is a frequent occurrence of a data breach that might present a difficult risk assessment when devices are no longer available.
5. **Mispostal** involves internal human error due to inattentiveness; there is no malicious action.
6. **Social engineering** refers to attacks involving identity theft and email exfiltration.

For each category of personal data breaches, the guidelines provide advisable, but not exclusive or comprehensive, practical measures and thus provide guidance for dealing with data breaches and future prevention.

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

5.1.2. Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive

See Section 3.2.1 for the full summary.

The EDPB issued recommendations to provide guidance to the European Commission on the level of data protection in third countries and international organisations under the Law Enforcement Directive (LED). It establishes the core data protection principles that have to be present in a third country's legal framework or an international organisation to ensure essential equivalence with the EU framework within the scope of the LED. In addition, it may guide third countries and international organisations interested in obtaining adequacy. The finding of an adequate level of data protection does not require a demonstration of a point-by-point mirroring of EU legislation, but rather the effectiveness of the core requirements of legislation in a third country (i.e. enforced and followed in practice).

Adopted: 2 February 2021; formatting changes made on 6 July 2021

5.1.3. Guidance Addendum on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Arts. 42 and 43 GDPR)

The EDPB expanded the framework on certification criteria by adopting this guidance that supplements Guidelines 01/2018 on certification and identifying certification criteria according to Arts. 42 and 43 GDPR (Guidelines 1/2018) and Guidelines 04/2018 on the accreditation of certification bodies under Art. 43 GDPR (2016/679). The improvement of certain aspects of Guidelines 01/2018 aims at assisting stakeholders involved in the drafting of certification criteria in the context of GDPR certification as well as helping SAs and the EDPB in providing consistent evaluation with regard to certification criteria approval.

Scheme owners that intend to submit a certification scheme may be required to commence early informal engagement with the competent SA, which will aid the preparations and clarify the expectations on the scheme.

Controllers or processors may apply for certification of processing activities that involve personal data, however, GDPR certification cannot be provided for standalone products.

All certification schemes shall have a clearly defined scope while indicating what is not permissible, in order to avoid "scope creep". The scope has to be practical, tractable and provide an added value.

Certification is not about stating an entity is 100% GDPR compliant, but instead aims to show, regarding a concrete Target of Evaluation and its processing operations, that the applicant made everything possible to satisfy certification criteria. The guidance outlines in detail the proper framing of certification criteria and the elements that should be taken into account with regard to certification criteria updates.

Adopted: 6 April 2021 and adopted in its final version following public consultation on 14 December 2021

5.1.4. Guidelines 02/2021 on virtual voice assistants

Recent technological advances have greatly increased the accuracy and popularity of virtual voice assistants (VVA). Among other devices, VVAs have been integrated in smartphones, connected vehicles, smart speakers and smart TVs.

A VVA is a service that has the capacity to understand and execute voice requests, as well as to mediate with other IT systems if necessary. Crucial to a VVA's nature is the access and processing of a huge amount of personal data that carries important data protection implications. The EDPB adopted these guidelines in order to advise relevant stakeholders on how to address the most relevant data protection and privacy compliance challenges for VVAs.

The EDPB provides guidance on appropriate legal basis for four of the most common purposes for processing personal data by VVAs: the execution of user requests, the improvement of the VVA machine learning model, biometric identification, and profiling for personalised content or advertising. In this respect, in addition to the GDPR, the Directive on Privacy and Electronic Communications (ePrivacy Directive) has to be considered. Based on its Art. 5(3), prior consent of a user would be necessary for the storing or gaining of access to information for any purpose other than executing a user's request.

The guidelines also give advice on transparency requirements and recall that, even when it comes to screenless devices, VVA providers must inform users according to the GDPR when setting up the VVA installation or using a VVA app for the first time. All users should also be able to exercise their rights through voice commands. Further, the guidelines

include a list of recommendations on such matters as processing of children's data and sensitive data, as well as on data deletion and data security.

Adopted: 9 March 2021 and adopted in its final version following public consultation on 7 July 2021

5.1.5. Guidelines 03/2021 on the application of Art. 65(1)(a) GDPR

Art. 65(1)(a) GDPR is a dispute resolution mechanism provided by the EDPB in case of dispute between SAs relating to the enforcement activities in the framework of a One-Stop-Shop (OSS) procedure. It is designed to guarantee the GDPR's correct and consistent application in circumstances involving cross-border processing of personal data.

This mechanism aims at settling conflicting views arising on the merits of a case between the Lead Supervisory Authority (LSA) and Concerned Supervisory Authorities (CSAs) who have lodged relevant and reasoned objections on a draft decision.

The EDPB elaborates on the application of relevant provisions of the GDPR and the EDPB Rules of Procedure, lays out an outline of the main stages of the procedure and clarifies its competence when adopting a legally binding decision under Art. 65(1)(a) GDPR. The guidelines also include an overview of the applicable procedural safeguards (such as the right to be heard, access to the file and the duty to give reasons).

Adopted: 13 April 2021

5.1.6. Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions

The continuous development of the digital economy and e-commerce has increased the number of online transactions. This increase heightens the risk of fraud associated with the use of credit card data online. Against this background, the EDPB has issued recommendations clarifying the legal basis for the storage of credit card data by online providers of goods and services, for the sole and specific purpose of facilitating further purchases by data subjects. These recommendations cover situations in which data subjects buy a product or pay for a service via a website or an application and provide their credit card data in order to conclude a unique transaction.

In such situations, consent (Art. 6(1)(a) GPDR) appears to be the sole appropriate legal basis for storing credit card data for future purchases. The controller should ensure that the data subject provides GDPR-standard consent to store the credit card data after a purchase. The consent must be freely given, specific, informed and unambiguous. It must be delivered by a clear affirmative action and should be requested in a user-friendly way, such as through a checkbox that is not pre-ticked. Additionally, it must be distinguished from the consent given for terms of service or sales and it cannot be a condition to the completion of a transaction.

In accordance with Art. 7(3) GDPR, data subjects have the right to withdraw their consent for the storing of credit card data for the purposes of facilitating further purchases at any time. Such withdrawal must be free, simple and as easy for the data subject as it was to give consent. As a consequence of a withdrawal, the controller must effectively delete the credit card data stored for the sole purpose of facilitating further online transactions.

Adopted: 19 May 2021

5.1.7. Guidelines 04/2021 on codes of conduct as tools for transfers

The EDPB expanded the general framework for the adoption of codes of conduct (CoCs) provided under Guidelines 1/2019

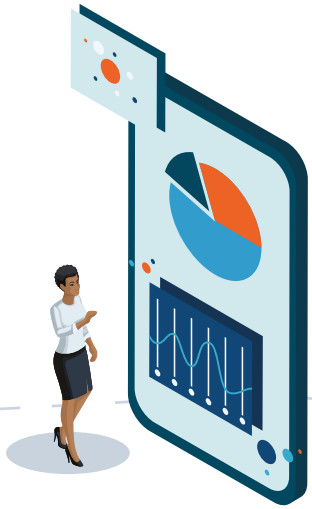
on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 by adopting these complementary guidelines. Their main purpose is to specify the application of Art. 40(3) and Art. 46(2)(e) GDPR relating to CoCs as appropriate safeguards for transfers of personal data to third countries. These GDPR provisions stipulate that a valid CoC may also be adhered to and used by controllers and processors not subject to the GDPR to provide appropriate safeguards for transfers of personal data outside of the EEA.

The CoC must be accompanied by a legally binding instrument, whereby the data importer commits to comply with the obligations set forth in the CoC, in order to ensure that the transferred personal data remains adequately protected, as per GDPR standards, when transferred outside the EEA. From a content perspective, the CoC should provide appropriate safeguards that include (1) essential principles, rights and obligations under the GDPR and (2) guarantees specific to the context of the transfer.

The guidelines include a checklist of minimum elements that a transfer CoC should include, which, depending on the transfer scenario, may need to be supplemented with additional commitments and measures.

In terms of the adoption process, the parties submitting a transfer CoC for approval must obtain the approval decision of the CSA following a favourable opinion from the EDPB and an implementing decision by the European Commission giving general validity to the CoC.

Adopted: 7 July 2021



5.1.8. Guidelines 05/2021 on the Interplay between the application of Art. 3 and the provisions on international transfers as per Chapter V of the GDPR

To clarify the interplay between the territorial scope of Art. 3 GDPR and the provisions on international transfers in Chapter V of the GDPR, the EDPB's guidance provides a consistent interpretation of the concept of international transfers. It aims to assist controllers and processors with identifying whether a processing operation constitutes an international transfer.

There are three cumulative criteria that must be met for data processing to be classified as a transfer:

1. A controller or processor ("exporter") is subject to the GDPR for the given processing;
2. This controller or processor transmits or makes available the personal data to another controller, joint controller or processor; and
3. This other controller, joint controller or processor is in a third country or is an international organisation ("data importer"), irrespective of whether or not the importer is already subject to the GDPR under Art. 3 GDPR.

The EDPB clarifies that disclosure of data made directly available by individuals and on their own initiative, are not transfers as there is no data exporter, meaning a controller or processor sending the data abroad.

If the identified criteria are not met, there is no transfer and Chapter V of the GDPR does not apply.

Adopted: 18 November 2021

5.1.9. Guidelines adopted after public consultation

5.1.9.1. Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679

To clarify the OSS cooperation mechanism for SAs outlined in the GDPR, the EDPB guidance establishes a common understanding of the notion of a "relevant and reasoned" objection, on the basis of the definition enshrined in Art. 4(24) GDPR, and addresses its interpretation.

Under the OSS cooperation mechanism, and specifically under Art. 60(3) and (4) GDPR, an LSA is required to submit a draft decision to the CSAs, who may then raise a "relevant and reasoned objection" within a set timeframe. In this context, the EDPB further clarifies the meaning of each of the elements of the definition in Art. 4(24) GDPR.

The guidelines explain that in order for an objection to be "relevant", there should be a direct connection between the substance of the draft decision at hand and the objection, since the objection, if followed, would entail a change to the draft decision leading to a different conclusion. The EDPB further clarifies that the objection needs to concern either whether there is an infringement of the GDPR or whether the envisaged action towards the controller or processor complies with the GDPR.

The objection will be adequately "reasoned" when it is clear, precise, coherent and detailed in explaining the reasons for objection, through legal or factual arguments. The EDPB also provides clarification on the obligation for the CSAs to clearly demonstrate in their objection the significance of the risks posed by the draft decision for the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data.

The first version of the guidelines was adopted on 8 October 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 9 March 2021

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

As they move into our everyday lives, connected vehicles have become a significant subject for regulators, particularly as they require personal data processing within a complex ecosystem.

The guidelines focus on the processing of personal data in relation to the non-professional use of connected vehicles. They clarify key privacy and data protection risks, including the security of personal data, ensuring full control over the processing, the appropriate legal basis for the processing and how GDPR-compliant consent should be collected.

To help controllers mitigate the risks for data subjects, the EDPB identifies three categories of personal data requiring special attention:

1. **Location data**, which has a particularly sensitive nature, due to it possibly revealing life habits;
2. **Biometric data**, for which special protection is provided in Art. 9 GDPR;
3. **Data revealing criminal offences** and other infractions, whose processing is subject to the safeguards contained in Art. 10 GDPR.

The EDPB also highlights the interplay between the GDPR and the ePrivacy Directive, noting that the connected vehicle and any device connected to it should be considered "terminal equipment" for the purposes of Art. 5(3) of the ePrivacy Directive. It further outlines the considerations to be taken for a lawful processing under the two instruments.

Lastly, the EDPB presents multiple case studies, such as "pay as you drive" insurance schemes, automatic emergency calls and accidentology studies.

The first version of the guidelines was adopted on 28 January 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 9 March 2021

5.1.9.3. Guidelines 08/2020 on the targeting of social media users

As mechanisms used to target social media users become more sophisticated and an increasingly large number of data sources are combined and analysed for targeting purposes, the topic has gained increased public interest and regulatory scrutiny.

Within this environment, the EDPB identifies three key actors:

1. **Users**: individuals who make use of social media;
2. **Social media providers**: providers of an online service that enables the development of networks of users;
3. **Targeters**: natural or legal persons that use social media services to direct specific messages to users.

Referring to relevant case law of the CJEU, such as the judgments in Case C-40/17 (*Fashion ID*), Case C-25/17 (*Jehovah's Witnesses*) and Case C-210/16 (*Wirtschaftsakademie*), the EDPB provides specific examples to clarify the roles of targeters and social media providers within different targeting mechanisms. Social media providers and targeters are often identified as joint controllers for the purposes of Art. 26 GDPR.

When it comes to targeting social media users, they may be targeted on the basis of provided, observed or inferred data, as well as a combination thereof.

There are numerous risks posed to the rights and freedoms of individuals as a result of processing personal data, including the possibility of discrimination and exclusion, and the potential for manipulating and influencing users. In this context, the EDPB highlights the relevant transparency requirements, the right of access and the joint controllers' duty to conduct a Data Protection Impact Assessment if the processing operations are "likely to result in a high risk" to the rights and freedoms of data subjects.

The first version of the guidelines was adopted on 2 September 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 13 April 2021

5.1.9.4. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

In its judgment in Case C-311/18 (*Schrems II*), the CJEU reaffirmed that the protection granted to personal data in the EEA must travel with the data wherever it goes. The level of protection in third countries does not need to be identical to that guaranteed within the EEA, but essentially equivalent. According to the CJEU, data exporters may implement supplementary measures to fill gaps in protection and bring it up to the level required by EU law, where Art. 46 GDPR transfer tools cannot guarantee it by themselves. The EDPB issued recommendations on 10 November 2020 that provide data exporters with a series of six steps to follow to apply the principle of accountability to data transfers, and some examples of supplementary measures. Updates were included in the guidelines in 2021 following the public consultation.

Adopted: 18 June 2021

5.1.9.5. Guidelines 07/2020 on the concepts of controller and processor in the GDPR

This updated EDPB guidance builds upon and replaces the Article 29 Working Party Opinion 01/2010 on the concepts of "controller" and "processor" (WP169). The correct interpretation of the concepts of controller, joint controller and processor have been crucial in the application of the GDPR, since these actors determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice.

Following the public consultation, the EDPB further elaborated upon its guidance, adding clarifications on, amongst others, the distinction between essential and non-essential means, issues concerning joint controllership and processors' roles in relation to data breaches.

The first version of the guidelines was adopted on 2 September 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 7 July 2021

5.1.9.6. Guidelines 10/2020 on restrictions under Art. 23 GDPR

The GDPR allows for data subject rights to be restricted in exceptional circumstances. The EDPB adopted the final version of its guidance with regards to restrictions of data subject rights under Art. 23 GDPR. The guidelines recall the conditions surrounding the use of such restrictions in light of the EU Charter of Fundamental Rights and the GDPR. They provide a thorough analysis of the criteria to apply restrictions, the assessments that must be observed, how data subjects can exercise their rights after the restrictions are lifted, and the consequences of infringing Art. 23 GDPR.

The first version of the guidelines was adopted on 15 December 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 13 October 2021

5.2. CONSISTENCY OPINIONS

5.2.1. Opinions on draft decisions regarding Binding Corporate Rules

SAs may approve Binding Corporate Rules (BCRs) within the meaning of Art. 47 GDPR. BCRs are data protection policies implemented and adhered to within a group of enterprises established in the EEA for transfers of personal data outside the EEA within the same group. In 2021, several SAs submitted their draft decisions regarding the controller or processor

BCRs of various companies to the EDPB, requesting an opinion under Art. 64(1)(f) GDPR. The EDPB issued eighteen opinions on BCRs.

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

The various opinions are listed below:

- Opinion 01/2021 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Saxo Bank Group Adopted: 22 January 2021
- Opinion 02/2021 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Elanders Group Adopted: 22 January 2021
- Opinion 03/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of BDO Adopted: 22 January 2021
- Opinion 04/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of BDO Adopted: 22 January 2021
- Opinion 06/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of Kumon Group Adopted: 16 February 2021
- Opinion 07/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Kumon Group Adopted: 16 February 2021
- Opinion 08/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Processor Binding Corporate Rules of Luxoft Group Adopted: 16 February 2021
- Opinion 09/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Controller Binding Corporate Rules of Luxoft Group Adopted: 16 February 2021
- Opinion 21/2021 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the CGI Group Adopted: 1 July 2021
- Opinion 22/2021 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the CGI Group Adopted: 1 July 2021
- Opinion 26/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Controller Binding Corporate Rules of the Internet Initiative Japan Group Adopted: 2 August 2021
- Opinion 27/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Processor Binding Corporate Rules of the Internet Initiative Japan Group Adopted: 2 August 2021
- Opinion 28/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Oregon Tool, Inc (formerly “Blount”) Adopted: 2 August 2021
- Opinion 29/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of Oregon Tool, Inc (Formerly “Blount”) Adopted: 2 August 2021
- Opinion 30/2021 on the draft decision of the Spanish

Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group Adopted: 2 August 2021

- Opinion 31/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group Adopted: 2 August 2021
- Opinion 33/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Carrier Adopted: 26 October 2021
- Opinion 34/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Otis Adopted: 26 October 2021

5.2.2. Opinions on draft requirements for accreditation of a certification body

Seven SAs submitted their draft decisions on accreditation requirements for certification bodies under Art. 43(1)(b) GDPR to the EDPB, requesting an opinion under Art. 64(1)(c) GDPR.

These requirements allow the accreditation of certification bodies responsible for issuing and renewing certification in accordance with Art. 42 GDPR.

These opinions aim to establish a consistent and harmonised approach regarding the requirements that SAs and national accreditation bodies apply when accrediting certification bodies under the GDPR. To do so, the EDPB made several recommendations and encouragements to the relevant SAs on the amendments to be made to the draft accreditation requirements.

The SAs then amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various opinions are listed below:

- Opinion 12/2021 on the draft decision of the competent Supervisory Authority of Portugal regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 20 July 2021
- Opinion 13/2021 on the draft decision of the competent Supervisory Authority of Romania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 23 March 2021
- Opinion 19/2021 on the draft decision of the competent Supervisory Authority of Hungary regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 1 June 2021
- Opinion 25/2021 on the draft decision of the competent Supervisory Authority of Lithuania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 20 July 2021
- Opinion 35/2021 on the draft decision of the competent Supervisory Authority of Belgium regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted 30 November 2021
- Opinion 36/2021 on the draft decision of the competent Supervisory Authority of Norway regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted 30 November 2021
- Opinion 38/2021 on the draft decision of the competent Supervisory Authority of Latvia regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted 20 November 2021

5.2.3. Opinions on SAs' approval of accreditation requirements for code of conduct monitoring body

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

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

The various opinions are listed below:

- Opinion 10/2021 on the draft decision of the competent Supervisory Authority of Hungary regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 March 2021
- Opinion 11/2021 on the draft decision of the competent Supervisory Authority of Norway regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 March 2021
- Opinion 23/2021 on the draft decision of the competent Supervisory Authority of Czech Republic regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 20 July 2021
- Opinion 24/2021 on the draft decision of the competent Supervisory Authority of Slovakia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 20 July 2021
- Opinion 37/2021 on the draft decision of the competent Supervisory Authority of Malta regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted 30 November 2021

5.2.4. Opinion on SAs' draft Standard Contractual Clauses

Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA (Art. 28(8) GDPR)

The contract or other legal act to govern the relationship between the controller and the processor in accordance with Art. 28(3) GDPR may be based, in whole or in part, on Standard Contractual Clauses (SCCs).

An SA may adopt SCCs in accordance with the consistency mechanism. As such, the EDPB reviews draft SCCs submitted by SAs to contribute to the consistent application of the GDPR throughout the EEA. In March 2021, the Lithuanian SA (LT SA) submitted its draft SCCs to the EDPB, requesting an opinion under Art. 64(1)(d) GDPR. The EDPB held that the draft SCCs needed some further adjustments and proposed several recommendations and encouragements on how to amend them.

Adopted: 19 May 2021

5.2.5. Opinions on SAs' approval of codes of conduct

Two SAs submitted their draft decisions on the approval of two codes of conduct that related to processing activities in several Member States. The codes of conduct were reviewed in accordance with the procedures set up by the EDPB in Guidelines 04/2021 on codes of conduct and in the EDPB Document on the procedure for the development of informal "Codes of Conduct sessions". Those codes of conduct do not aim to be used as a tool for international transfer of data (Art. 46(2)(e) GDPR).

The EDPB considered that the draft codes complied with the GDPR as they fulfilled the requirements imposed by Art. 40 and Art. 41 GDPR. The EDPB also recalled that, in accordance with Art. 40(5) GDPR, the competent SA would have to submit the code of conduct to the EDPB in case of amendment or extension.

The various opinions are listed below:

- Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe Adopted: 19 May 2021
- Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE) Adopted: 19 May 2021

5.2.6. Opinion on SAs' authorisation of administrative arrangements

Opinion 05/2021 on the draft Administrative Arrangement for the transfer of personal data between the Haut Conseil du Commissariat aux Comptes (H3C) and the Public Company Accounting Oversight Board (PCAOB)

The Haut Conseil du Commissariat aux Comptes submitted a draft Administrative Arrangement for the transfers of personal data between the Haut Conseil du Commissariat aux Comptes and the Public Company Accounting Oversight Board to the French SA, which thereafter requested an opinion from the EDPB pursuant to Art. 64(2) GDPR.

The EDPB welcomed the efforts made for this Administrative Agreement, which included a number of important data protection safeguards in line with the GDPR as well as with the safeguards laid down in EDPB Guidelines 02/2020, and underlined some key considerations.

Adopted: 2 February 2021

5.2.7. Opinion on the legal basis for an SA to order ex officio data erasure

Opinion 39/2021 on whether Art. 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject.

The Hungarian SA requested the EDPB to issue an opinion on whether Art. 58(2)(g) GDPR could serve as a legal basis for an SA to order ex officio the erasure of unlawfully processed personal data, in a situation where such a request was not submitted by the data subject. The EDPB concluded that Art. 58(2)(g) was a valid legal basis in such a situation.

Adopted: 14 December 2021

5.3. BINDING DECISIONS

5.3.1. Binding Decision 01/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Art. 65(1)(a) GDPR

See Section 3.5 for a full summary.

In relation to the draft decision regarding WhatsApp Ireland (WhatsApp IE) of the Irish SA and the subsequent CSA objections, the EDPB adopted a binding decision under Art. 65(1)(a) GDPR. The decision concludes that the Irish SA should amend its draft decision regarding infringements of transparency, the period to bring processing operations into compliance and the calculation of the fine.

Adopted: 28 July 2021

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

See Section 3.6 for a full summary.

Following a request from the Hamburg SA, which had taken provisional measures, in accordance with Art. 66(1) GDPR, against Facebook Ireland Ltd. (Facebook IE) banning their processing of WhatsApp IE user data in Germany for their own purposes, the EDPB adopted an urgent binding decision under Art. 66(2) GDPR.

The decision states that the conditions to prove the existence of an infringement and urgency were not met. The decision concludes that there is a high likelihood that Facebook IE already processes WhatsApp IE user data as a (joint) controller for a number of purposes, which could not be demonstrated with certainty due to contradictions, ambiguities and uncertainties noted in the evidence provided. Due to the high likelihood of infringements of the GDPR, the decision requests the Irish SA to carry out, as a matter of priority, a statutory investigation to determine whether such processing activities are taking place or not, and if it is the case, whether they have a proper legal basis under GDPR.

Adopted: 12 July 2021

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

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

All the decisions added in 2021 are related to decisions made by the SAs following the EDPB consistency opinions or following the 01/2021 EDPB binding decision regarding a dispute on an Irish SA draft decision on WhatsApp.

See Section 5.2 on consistency opinions and Section 5.3 on binding decisions.

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

5.5.1. Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom

See Section 3.2.2 for a full summary.

When providing an assessment of the draft implementing decision on the adequacy of personal data protection offered by the UK under the GDPR, the EDPB finds that, as the UK is a former EU Member State, many aspects of the UK's data protection framework are essentially equivalent to those in the EU. However, there are several potential challenges with essential equivalence of UK and EU data protection law and the European Commission should monitor future developments.

5.5.2. Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom

See Section 3.2.3 for a full summary.

The EDPB recognises that many aspects of UK's data protection framework are essentially equivalent to the protections offered in the EU. Mindful of the possibility that the UK deviates in the future from the EU data protection framework, the EDPB welcomes the addition of a sunset clause into the draft decision. In addition, it further emphasises the importance of the European Commission in monitoring the developments of UK's data protection framework and, if after the adoption of the adequacy decision the adequate level of protection is no longer ensured, in taking actions by suspending, amending or repealing the adequacy decision.

5.5.3. Opinion 20/2021 on Tobacco Traceability System

On 3 March 2021, the European Commission requested the opinion of the EDPB, on the basis of Art. 70(1)(b) GDPR, on three questions related to the different roles of the actors involved in the tobacco traceability system established under Directive 2014/40/EU.

- First, the European Commission asked the EDPB whether it agrees with the European Commission's assessment according to which the Member States and the European Commission act as joint controllers with regard to the processing of personal data in the context of the EU tobacco traceability system. The EDPB considers that the European Commission has taken into consideration the necessary elements to perform the assessment of joint controllership. To achieve the purpose of monitoring compliance with and enforcing the rules, all the means identified (i.e. the ID Issuers' registries and the repositories) were necessary, since otherwise the traceability of tobacco products would not be possible and thus the purpose of processing would not be achievable.

- Second, the European Commission asked whether the EDPB agrees with the European Commission's assessment according to which the ID Issuers act as processors of the Member States. In response, the EDPB holds that the European Commission has not taken into consideration all the necessary elements to perform the assessment on the role of the ID Issuers. In this regard, it should be noted that, in case of joint controllership, the mere fact that the ID Issuers are appointed by the Member State, does not necessarily imply that they are only processors of the Member State.
- Third, the European Commission asked whether the EDPB agrees with the European Commission's assessment according to which the independent third parties hosting the primary repositories act as sub-processors of the operator of the secondary repository acting as a processor on behalf of the joint controllers (European Commission and the Member States). The EDPB states that the European Commission has taken into consideration the necessary elements to perform the assessment on the role of the providers of the primary repository.

The EDPB considerations regarding the European Commission's questions are without prejudice to any specific further assessment pursuant to applicable data protection legislation carried out by the controller as part of its obligations or by a competent SA in the exercise of its powers.

Adopted: 18 June 2021

5.5.4. Opinion 32/2021 regarding the European Commission draft implementing decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea

On 16 June 2021, the European Commission launched the formal process towards the adoption of its draft implementing decision on the adequate protection of personal data in the Republic of Korea under the Personal Information Protection Act pursuant to Art. 45 GDPR.

On the same date, the European Commission asked for the opinion of the EDPB in accordance with Art. 70(1)(s) GDPR. The EDPB assessed the level of protection afforded in the Republic of Korea on the basis of the draft decision itself, as well as on the documentation made available by the European Commission.

The EDPB assessed both the general GDPR aspects of the draft decision and the access by public authorities to personal data transferred from the EEA for the purposes of law enforcement and national security, including the legal remedies available to individuals in the EEA. The EDPB also assessed whether the safeguards provided under the South Korean legal framework are in place and effective.

The EDPB recognises that key aspects of South Korea's data protection framework are essentially equivalent to the protections offered in the EU, and welcomes the notifications adopted by the South Korean data protection authority, which provide relevant clarifications on some important safeguards considered within the adequacy assessment. The EDPB identifies some aspects to be further clarified and closely monitored by the European Commission.

Adopted: 24 September 2021

5.5.5. EDPB-EDPS Joint Opinion 01/2021 on standard contractual clauses between controllers and processors

On 12 November 2020, the European Commission published a draft Implementing Decision on Standard Contractual Clauses (SCCs) between controllers and processors for the matters referred to in Art. 28(3) and (4) GDPR and Art. 29(7) of Regulation (EU) 2018/1725 as well as a draft Annex containing the draft SCCs.

The European Commission requested a joint opinion of the EDPB and the EDPS on the basis of Art. 42(1) and (2) of Regulation (EU) 2018/1725 on this set of draft SCCs.

The joint opinion aims at ensuring consistency and a correct application of Art. 28 GDPR as regards the presented draft clauses that could serve as SCCs in compliance with Art. 28(7) GDPR and Art. 29(7) of Regulation (EU) 2018/1725.

The joint opinion comprises (i) a core part detailing general comments made by the EDPB and the EDPS and (ii) an annex where comments of a more technical nature were made directly to the Draft Decision and the Draft SCCs to provide some examples of possible amendments with the aim of bringing more clarity to the text and ensuring its practical usefulness in day-to-day operations of controllers and processors. The EDPB and the EDPS commented, inter alia, on the interplay with the other set of European Commission draft SCCs on transfers (see Section 5.5.6 below), the so-called "docking clause", which allows additional entities to accede to the SCCs, and other aspects relating to obligations for processors. Additionally, the EDPB and EDPS suggest that the Annexes to the SCCs clarify as much as possible the roles and responsibilities of each of the parties with regard to each processing activity.

Adopted: 14 January 2021

5.5.6. EDPB-EDPS Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries

On 12 November 2020, the European Commission requested the EDPB and the EDPS to issue a joint opinion on its draft implementing decision on SCCs for the transfer of personal data to third countries (joint opinion), in compliance with Art. 42(2) of Regulation (EU) 2018/1725. These draft SCCs aimed at updating and replacing the previous sets of SCCs adopted by the European Commission based on Directive 95/46/EC.

The joint opinion comprises (i) a core part detailing general comments and (ii) an annex with additional comments of a more technical nature made directly to the draft SCCs to provide some examples of possible amendments.

Overall, the EDPB and the EDPS note with satisfaction that the draft SCCs present a reinforced level of protection for data subjects, in particular, the specific provisions intending to address some of the main issues identified in the CJEU ruling in Case C-311/18 (Schrems II) and to reflect several measures identified in EDPB Recommendations 01/2020 on supplementary measures.

The EDPB and the EDPS also welcome the fact that this draft brings the previous SCCs in line with new GDPR requirements, and better reflects the widespread use of new and more complex processing operations often involving multiple data importers and data exporters, long and complex processing chains, as well as evolving business relationships.

The EDPB and EDPS consider that several provisions of the draft SCCs could be improved or clarified, such as the scope of the SCCs, certain third-party beneficiary rights, certain obligations regarding onward transfers, aspects of the assessment of third country laws regarding access to public data by public authorities, and the notification to the SA.

Adopted: 14 January 2021

5.5.7. EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)

On 25 November 2020, the European Commission requested a joint opinion of the EDPB and the EDPS, on the basis of Article 42(2) of Regulation (EU) 2018/1725, on the Proposal for the Data Governance Act (the Proposal).

The EDPB and the EDPS highlight that the Proposal is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. The scope of the opinion is limited to aspects of the Proposal related to the protection of personal data, which, as observed, represents a key - if not the most important - aspect of the Proposal.

The EDPB and the EDPS point out inconsistencies with the EU data protection legislation (as well as with other EU legislation, such as the Open Data Directive) and problems of the Proposal, which raises a significant number of serious concerns, often intertwined, related to the protection of the fundamental right to the protection of personal data. The EDPB and the EDPS provide advice and recommendations to the co-legislators to ensure in particular: legal certainty for natural persons, economic operators and public authorities; due protection of personal data for data subjects in line with the Treaty on the Functioning of the EU (TFEU), the EU Charter of Fundamental Rights and the data protection acquis; and a sustainable digital environment including the necessary "checks and balances".

Overall, the EDPB and the EDPS note that the Proposal, also having regard to the Impact Assessment accompanying it, does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law. The EDPB and the EDPS consider that this policy trend toward a data-driven economy framework without sufficient consideration of personal data protection aspects raises serious concerns from a fundamental rights viewpoint.

The EDPB and the EDPS furthermore highlight that the European Union model relies on the mainstreaming of its values and fundamental rights within its policy developments, and that the GDPR must be considered as a foundation on which to build a European data governance model. The EU legal framework in the field of personal data protection shall be considered as an enabler, rather than an obstacle, to the development of a data economy that corresponds to the Union values and principles.

Adopted: 10 March 2021

5.5.8. EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID 19 pandemic (Digital Green Certificate)

The EDPB and the EDPS note that the Proposal for a Regulation concerning the Digital Green Certificate aims at facilitating the exercise of the right to free movement within the EU during the COVID-19 pandemic by establishing a common framework, thus requiring all EU Member States to use the

Digital Green Certificate framework and issue certificates for that purpose.

The EDPB and the EDPS consider it essential to ensure that the Proposal is consistent and does not conflict in any manner with the application of the GDPR. Compliance with the principles of necessity and proportionality by the measures introduced with the Proposal should be carefully analysed. In this regard, the EDPB and EDPS underline the lack of an impact assessment accompanying the Proposal, which would provide substantiation of the impact of the measures and the effectiveness of already existing, less intrusive measures. They also underline that the Proposal must not lead to the creation of any sort of personal data central database at EU level under the pretext of the establishment of the Digital Green Certificate framework. Furthermore, the joint opinion includes specific comments about the categories of personal data, the adoption of adequate technical and organisational privacy and security measures, the identification of controllers and processors, the transparency and data subject's rights, the data storage and the international data transfers.

The Proposed Regulation did not address the use of the Digital Green Certificate framework at national level for other reasons than facilitating the free movement between EU Member States. In this regard, the Proposal may not be used as a legal basis for such further use. The EDPB and the EDPS also remark that any possible further use of the framework, the Digital Green Certificate and personal data related to it at the Member States level must respect Art. 7 and Art. 8 of the EU Charter of Fundamental Rights and must comply with the GDPR, including Art. 6(4) GDPR. This implies the need for a proper legal basis in Member State law, complying with the principles of effectiveness, necessity, proportionality and including strong and specific safeguards.

Adopted: 31 March 2021

5.5.9. EDPB-EDPS Joint Opinion 05/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

See Section 3.4 for a full summary.

The European Commission presented its Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) on 21 April 2021. In their joint opinion, the EDPB and the EDPS welcome the concern of the legislator in addressing the use of artificial intelligence (AI) within the EU and stress the important data protection implications of the future regulation. Relevant issues include the following: the Proposal's scope, a risk-based approach, prohibited uses of AI, high-risk AI systems, governance and the European AI Board, and its interaction with the data protection framework.

Adopted: 18 June 2021

5.5.10. Statement 02/2021 on new draft provisions of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)

Following the previous EDPB contribution to the draft Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), the EDPB adopted a statement on the new draft provisions to provide its expertise with a view to ensuring that data protection matters are duly considered in the overall drafting process of the Additional Protocol.

The statement focuses on assessing draft provisions that have not been subject to previous stakeholder consultations, such as joint investigations and their respective teams, expedited disclosure of stored computer data in an emergency, and request for domain name registration information.

The EDPB notes that the new draft provisions are likely to affect the conditions for access to personal data in the EU for law enforcement purposes and, consequently, it calls on the relevant EU and national institutions to carefully scrutinise the ongoing negotiations. The goal of such action is to guarantee full consistency of the proposed Second Additional Protocol with the EU acquis in the field of personal data protection.

Adopted: 2 February 2021

5.5.11. Statement 03/2021 on ePrivacy Regulation

The EDPB adopted a statement on the draft ePrivacy Regulation where it welcomes the agreement on the negotiation mandate by the Council of the EU as a positive step in the finalisation of the ePrivacy Regulation. The statement expresses concerns about proposed rules on the retention of electronic communication data for the purposes of law enforcement and safeguarding national security. It further recalls the necessity of a specific EU regulation protecting the confidentiality of electronic communications. The upcoming Regulation must enforce the consent requirement for cookies and similar technologies, and enable technical tools allowing consent to be easily obtained.

The EDPB reiterates that competent national SAs responsible for enforcing the GDPR should be entrusted with the oversight of the privacy provisions of the future ePrivacy Regulation in order to ensure harmonised interpretation and enforcement of the ePrivacy Regulation across the EU and to guarantee a level playing field in the Digital Single Market. The EDPB also underlines the practical difficulties that will be faced in case national competent authorities who are not members of the EDPB would have to interact with the EDPB.

Adopted: 9 March 2021

5.5.12. Statement 04/2021 on international agreements including transfers

The EDPB calls upon the EU Member States to assess and, where necessary, review their international agreements that involve international transfers of personal data and were concluded before 24 May 2016 (for those relevant to the GDPR) and 6 May 2016 (for those relevant to the Law Enforcement Directive (LED)). These actions should be performed to ensure alignment, where needed, with EU law, in particular the GDPR and the LED, CJEU case law on data protection, and relevant EDPB guidance.

Adopted: 13 April 2021

5.5.13. EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime

The EDPB submitted comments on the draft Second Additional Protocol to the Council of Europe Cybercrime Convention Committee (T-CY) during its sixth consultation round.

From an EU data protection law point of view, the draft Protocol, as per its level of norm, provisions and legal effect, would be applicable to the disclosure and transfer of personal data from the EU to third countries. In relation to the draft Art. 13 of the Protocol ("Condition and safeguards"), the EDPB recommends that the application and implementation of the principle of proportionality be included in the text. The EDPB could not provide a full assessment on the draft text of Art. 14 ("protection of personal data") due to the non-publication of the explanatory report for this provision.

The EDPB recommends clarifying the application of some of the principles and procedures that Art. 14 contains, such as its scope, purpose and use of personal data received by the requesting party, the processing of sensitive data, retention periods, automated decisions, maintaining of records, onward sharing, onward transfer, transparency and notice, rights of data subjects, oversight and suspension.

The EDPB calls on the T-CY members and protocol drafters to amend the draft provisions presented for consultation to ensure the finalised protocol is fully compatible with EU primary and secondary law, guaranteeing that the level of protection of personal data as per EU law is not undermined.

Adopted: 4 May 2021

5.5.14. Statement 05/2021 on the Data Governance Act in light of the legislative developments

In pursuit of reinforcing its main remarks from the EDPB-EDPS Joint Opinion on the Data Governance Act (DGA) (see Section 5.5.7 for a full summary), the EDPB adopted this statement on the DGA concerning the developments in the legislative process.

The EDPB states that it is important to have robust data protection safeguards, as a lack of safeguards creates a risk that the trust in the digital economy would not be sustainable. There is a need to ensure consistency between the DGA and the EU data protection acquis. Certain aspects are particularly important, such as the provision in the DGA of a clear interplay between the DGA and the GDPR, the alignment of the definitions and terminology of the DGA with the ones of the GDPR, and the clarification of the appropriate legal basis regarding the processing of personal data.

Adopted: 19 May 2021

5.5.15. EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime

On 8 July 2020, the European Commission submitted to the EDPB a request focusing on health research and provided a list of concrete questions related to data protection for health related research.

In its replies, the EDPB states that ethics standards cannot be interpreted in such a way that only explicit consent of data subjects can be used to legitimise the processing of health data for scientific research purposes. Art. 6 and Art. 9 GDPR contain other options for a legal basis and an exemption, which can be relied on for processing of health data for scientific research purposes. In its replies the EDPB provides clarifications on data protection related concepts, such as the processing of previously collected health data, the notion of broad consent, transparency, data safeguards, large scale processing and international cooperation.

The EDPB response constitutes only a preliminary position on the topic. In its forthcoming guidelines on processing personal data for scientific research purposes, the EDPB will elaborate further on these issues while aiming at providing a more comprehensive interpretation of the various provisions in the GDPR that are relevant for the processing of personal data for scientific research purposes.

Adopted: 2 February 2021

5.6. OTHER GUIDANCE AND INFORMATION NOTES

5.6.1. Pre-GDPR BCRs overview list

The EDPB published an updated list of pre-GDPR BCRs on its website. This list provides information on BCRs that were

submitted to SAs in accordance with the rules applicable under Directive 95/46 and for which the procedure for approval ended prior to 25 May 2018, when the GDPR started applying. The list notes which SA took charge of coordinating the informal EU cooperation procedure. Inclusion in the list does not imply endorsement by the EDPB of these BCRs.

Adopted: 26 January 2021

5.6.2. Statement on the withdrawal of the United Kingdom from the European Union - update 13/01/2021

The second version of the Statement, adopted on 13 January 2021 (the first having been adopted on 15 December 2020), was updated taking into consideration that on 15 December 2020, an agreement on future relations was reached between the EU and the UK. The EDPB reminds all stakeholders that the agreement provides that, for a specified period and upon the condition that the UK's current data protection regime stays in place, all transfers of personal data between stakeholders subject to the GDPR and UK entities will not be considered as transfers to a third country subject to the provisions of Chapter V GDPR. This interim provision could be applied for a maximum period of six months (i.e. until 30 June 2021 at the latest). The EDPB specifies that, as of 1 January 2021, the One-Stop-Shop (OSS) mechanism is no longer applicable to the UK, so the UK Information Commissioner's Office is no longer part of it.

The EDPB emphasises that the decision to benefit from the unified dialogue enabled by the OSS mechanism in cross-border processing cases is up to the individual controllers and processors, who to that end could decide whether to set up a new main establishment in the EEA under the terms of Art. 4(16) GDPR. The EDPB recalls that controllers and processors not established in the EEA, but whose processing activities are subject to the application of the GDPR under Art. 3(2) GDPR, are required to designate a representative in the EU in accordance with Art. 27 GDPR.

Adopted: 13 January 2021

5.6.3. Information note on data transfers under the GDPR to the United Kingdom after the transition period - update 13/01/2021

By the time of the second version of the note, adopted on 13 January 2021, an agreement had been reached between the EU and the UK on 24 December 2020. The agreement provided that for a maximum period of six months from its entry into force – i.e. until 30 June 2021 at the latest - and upon the condition that the UK's current data protection regime stays in place, all flows of personal data between stakeholders subject to the GDPR and UK organisations would not be considered as international transfers.

Until 30 June 2021, at the latest, organisations subject to the GDPR would be able to carry on transferring personal data to UK organisations without the need to either put in place a transfer tool under Art. 46 GDPR or rely on an Art. 49 GDPR derogation. If no adequacy decision applicable to the UK as per Art. 45 GDPR would be adopted by 30 June 2021 at the latest, all transfers of personal data between stakeholders subject to the GDPR and UK entities would then constitute a transfer of personal data to a third country.

Adopted: 13 January 2021

5.7. PLENARY MEETINGS AND SUBGROUPS

In the period between 1 January and 31 December 2021, the EDPB held 15 plenary meetings. The agendas and minutes of these meetings are published on the EDPB website. The outcome of the plenary meetings consists of adopted guidelines, opinions and other documents such as statements

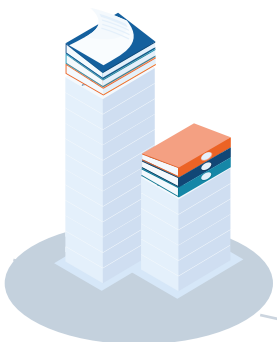
or information notes to advise the European Commission, national SAs and other stakeholders on data protection matters, with a primary focus on the GDPR. Additionally, there were 200 expert subgroup meetings. In total, 389 meetings were held, including plenary meetings, expert subgroup meetings and drafting team meetings.

The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks. Chapter 8 outlines the list of the expert subgroups and their respective mandates.

5.8. STAKEHOLDER CONSULTATION

5.8.1. Stakeholder events

The EDPB organises stakeholder events to gather input and views on specific issues in the interest of developing future guidance. In 2021, the EDPB organised such an event on processing personal data for scientific research purposes on 30 April. The event took place online and secured approximately 60 participants that represented a combination of academia, NGOs, commercial organisations and SAs. They shared their experience concerning the use of personal data for scientific research purposes and emphasised areas that needed further clarifying or explaining. Alongside this provided input, the EDPB gathered further valuable insights on the topic from a questionnaire sent to both parties who attended and could not attend prior to the event. The EDPB will use all the provided stakeholder input in the context of drafting future guidance on data processing for scientific research purposes.



5.8.2. Public consultation on draft guidance

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

To further enhance transparency, the EDPB publishes on its website stakeholders' contributions to public consultations. In 2021, the EDPB launched several such consultations:

- In January, the EDPB opened public consultations on Guidelines 01/2021 on Examples regarding Data Breach Notification. There were 32 contributions made to the guidelines, mostly submitted by business organisations and associations or DPO entities.
- In March, Guidelines 02/2021 on Virtual Voice Assistants were open for public consultations. They attained eighteen contributions from a mix of different entities, such as academic and research institutions and business associations.
- Later in April, the EDPB opened public consultations on both Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Arts. 42 and 43 of the Regulation) and Guidelines 03/2021 on the application of Art. 65(1)(a) GDPR. The Guidance on certification criteria assessment received contributions from six entities, mainly comprising individuals, academia and public authorities. The Guidelines 03/2021 on the application of Art. 65(1)(a) GDPR received three contributions from a variety of entities.
- The EDPB published Guidelines 04/2021 on codes of conduct as tools for transfers for consultation in July. There were ten contributions to these guidelines.

- In November, the EDPB launched public consultations on Guidelines 05/2021 on the Interplay between the application of Art. 3 and the provisions on international transfers as per Chapter V of the GDPR, which were accepting contributions until 31 January 2022.

5.8.3. Survey on practical application of adopted guidance

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

5.8.3.1. Participants and methodology

The survey compiles the views of various entities with different interests and concerns related to EU data protection law. Stakeholders consulted included representatives from an EU DPO organisation, representing a network of national associations of data protection and privacy officers. Accordingly, a representative and comprehensive view of the sector was obtained. Stakeholders also included academia and NGOs in the field of data protection and privacy rights. This allowed for a broad representation of actors from different sectors. The EDPB used semi-structured, one-on-one virtual interviews to consult participants. The questions were based on a standardised questionnaire. From this, data was synthesised and commonalities identified.

5.8.3.2. Findings

The surveyed stakeholders indicated that the EDPB guidelines and recommendations are generally coherent and helpful in interpreting ambiguous data protection rules and better understanding data protection rights and duties. The structure of the documents also provides for easy navigation through the content, with Guidelines 01/2021 on data breach notifications receiving praise in this respect.

Most stakeholders consulted the guidelines and recommendations on a near daily basis for work purposes.

Stakeholders indicated the need for quicker adoption of new guidelines and recommendations. In addition, they suggested that shorter documents with comprehensive executive summaries would be useful. When certain guidance documents become very long, a suggestion was made for the EDPB to consider issuing a complementary, shorter version of the final document. With respect to content, stakeholders saw high practical value in the examples outlined in the EDPB guidelines and hoped to see this practice continue.

The surveyed stakeholders actively participated in the consultative processes of the EDPB throughout 2021. Some participants suggested they would appreciate a clearer outline of how their proposed input was incorporated into guidelines adopted after consultation.

Overall, due to the improved website and consultation processes, the participants found significant improvement in the communication and transparency of the EDPB. Stakeholders stated that in light of consistency and compliance, they followed and acted in accordance with the EDPB's guidance.

The EDPB highly appreciates the stakeholders' participation and useful contribution to its work. Feedback on the guidance's operational value and alignment with other EU laws was equally appreciated as it gave actionable insights into stakeholder needs. The provided feedback on communication and transparency is also beneficial for future stakeholder engagement and initiating plans of action. Overall, the EDPB plans to continue upholding and building upon the consistency of its work in the future.

5.9. EXTERNAL REPRESENTATION OF THE BOARD

Public awareness and cooperation are vital to upholding data protection rights in the EEA and beyond, which is why the EDPB values stakeholder and citizen engagement. The EDPB Secretariat supports the Chair and Deputy Chairs in engagements with other EU institutions or bodies, and when they represent the EDPB at conferences and multi-stakeholder platforms. Staff members from the EDPB Secretariat also take part in several events to present the activities of the EDPB.

5.9.1. Participation of Chair and Deputy Chairs in conferences and speaking engagements

In 2021, the Chair of the EDPB, Andrea Jelinek, had over nineteen speaking engagements, which for the most part were remote. The speaking engagements included press briefings, presentations and panel discussions for a range of institutes, academic forums and policy agencies. The Chair also met with European Commissioners and representatives from, among others, UNESCO and the Council of the EU Working Party on Information Exchange and Data Protection. In addition, she participated in several conferences and summits on data protection and privacy matters.

The EDPB Deputy Chair Ventsislav Karadjov took part in nine speaking engagements, most of which were remote. They consisted of speeches, presentations and panel discussions at several conferences and forums. The EDPB Deputy Chair Aleid Wolfsen participated in three remote speaking engagements. His engagement comprised speeches, presentations and panel discussions at different events.

5.9.2. Participation of EDPB Staff in conferences and speaking engagements

EDPB staff represented the EDPB at 33 events, both in-person and remotely. The events were hosted by, amongst others, universities, trade associations and EU institutions. Their engagement at these events consisted of discussing achievements, challenges and potential solutions to current data protection issues, but also disseminating educational knowledge of data protection and privacy for tailored made courses at different universities.

6

SUPERVISORY AUTHORITY - ACTIVITIES IN 2021

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

These tools are:

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

6.1. CROSS-BORDER COOPERATION

The GDPR requires the EEA SAs to cooperate closely to ensure the consistent application of the GDPR and protection of individuals' data protection rights across the EEA.

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

6.1.1. Preliminary procedure to identify the Lead and Concerned Supervisory Authorities

Before starting a One-Stop-Shop (OSS) procedure for a cross-border case, it is necessary to identify the Lead Supervisory Authority (LSA) and the other Concerned Supervisory Authorities (CSAs). The LSA leads the investigation and drafts

the decision, while the CSAs have the opportunity to raise objections.

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

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

In case of conflicting views regarding which SA should act as LSA, the EDPB acts as a dispute resolution body and issues a binding decision. From 1 January 2021 to 31 December 2021, there were 553 instances in which LSAs and CSAs were identified.

6.1.2. Database regarding cases with a cross-border component

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

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

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

Please note that:

- References to case register entries in these statistics do not have a 1-to-1 correlation to the number of cross-border complaints handled per country as multiple complaints may be bundled in one case register entry which therefore can relate to multiple cross-border cases;

- Depending on the Member State legislation, supervisory authorities may have handled complaints outside of the Art 60 procedure in accordance with their national law.

6.1.3. One-Stop-Shop mechanism and decisions

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

The LSA must first investigate the case while taking into account national procedural rules, ensuring that the affected individuals can exercise their rights. The LSA can gather information from another CSA via mutual assistance or by conducting a joint investigation. The IMI system also gives the LSA and other CSAs at any point the opportunity to informally communicate with each other to collect and exchange relevant information.

Once the LSA has completed its investigation, it prepares a draft decision, which it then communicates to the CSAs. They have the right to object. An objection either leads to a revised draft decision or, if no route to consensus can be found, the EDPB acts as a dispute resolution body and issues a binding

decision. The LSA must adopt its final decision on the basis of the EDPB's decision. If the CSAs do not object to either the initial draft or the revised decision, they are deemed to agree with the draft decision.

Between 1 January 2021 and 31 December 2021, there were 209 draft decisions, which resulted in 141 final decisions.

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

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

The EDPB maintains a public register of the final decisions taken by LSAs and complaint receiving SAs pursuant to the OSS as a valuable resource to showcase how SAs work together to practically enforce the GDPR. The register offers an exceptional opportunity to read final decisions taken by, and involving, different SAs in a cross-border context. These decisions often contain important guidance on how to comply with the GDPR in practice. The register contains both final decisions and summaries prepared by the EDPB Secretariat and duly approved by SAs. The relevant SAs have validated the information in the register in accordance with the conditions provided by their national legislation.

This section contains a selection of examples of Art. 60 GDPR final decisions taken from the EDPB's public register. The first section contains some cases where SAs handed out administrative fines in accordance with Art. 83 GDPR when data controllers did not comply with the GDPR. The second section provides summaries of some other final decisions in cases where SAs did not issue administrative fines, but provided guidance on the interpretation of specific provisions of the GDPR.

The Annual Report references certain final decisions from 2021, but also includes one from late 2020.

6.1.3.1. Selection of cases involving administrative fines

Consistent enforcement of data protection rules is central to a harmonised data protection regime. Once an infringement of the GDPR has been established based on the assessment of the facts of the case, the competent SA must identify the most appropriate corrective measure to address the infringement. Administrative fines are one of the most powerful enforcement measures the SAs can adopt, together with the other measures in Art. 58 GDPR.

LSA: Dutch SA

Personal data breach / Notification of a personal data breach to the supervisory authority / Administrative fines

Year of decision: 2020[3]

OSS register number: EDPBI:NL:OSS:D:2020:173

On 7 February 2019, the service provider of an online platform notified the LSA of a personal data breach that it had discovered on 10 January 2019. The controller indicated in its notification that an unknown third party had gained access to personal data in the controller's reservation system which are used by the platform's partners to manage the reservations. As a result, the personal data of various data subjects who had made reservations via the controller's platform were compromised. The LSA then commenced an investigation on the controller's compliance with Art. 33(1) GDPR.

During its investigations, the LSA found that the controller had been informed on 8 January 2019 by one of its partners that, following a possible personal data breach in the reservation system, an unknown third party had contacted customers and pretended to be affiliated with the controller, once as an

employee of the controller and other times as an employee of one of the partner organisations on the platform. The LSA noted that the controller received two similar complaints from the same provider on 13 January 2019 and 20 January 2019; and that on 20 January 2019, a second partner reported the same type of incident. The LSA noted that, despite the reports about these several incidents, the controller's entity in charge of the receipt of these incidents did not notify the controller's security team until 31 January 2019. After having conducted investigations, the controller's security team informed the controller's privacy team on 4 February 2019.

In view of the circumstances in which the incidents were reported to the controller by the partners, the LSA found that the controller was deemed to have knowledge of the personal data breach at least on 13 January 2019, as the information given by the partner indicated with a reasonable degree of certainty that personal data had been compromised. As a result, the LSA pointed out that the controller should have notified the LSA of the personal data breach by 16 January 2019 at the latest. It is an established fact that the controller only made this notification on 7 February 2019, i.e. 22 days too late. The same applies if 20 January 2019 should be adopted as the starting date, then the notification was done 15 days too late compared to the deadline of 72-hour set out by Art. 33(1) GDPR.

The LSA stressed that the controller's argument that the delay in notifying the data breach was due to a failure by a single part of the controller's organisation to report the incident to the security team, as per the controller's internal procedure, is without effect. The LSA also stressed that, by choosing to carry out an in-depth investigation instead of notification in phases, the controller did not comply with the rules laid down in Art. 33(3) GDPR.

The controller had informed and advised the data subjects about taking measures to reduce the potential damage. The controller had declared itself willing to compensate any damages (suffered or to be suffered) by the data subjects. The controller also immediately informed its affected partners and placed warnings on the website.

The LSA imposed an administrative fine of EUR 475,000 on the controller for the infringement of Art. 33(1) GDPR.

[3]. Decision adopted in late 2020, so included in 2021 Annual Report.

LSA: Dutch SA

Personal data breach / Data security / Administrative fines

Year of decision: 2021

OSS register number: not available yet

On 24 October 2019, the LSA received a notification from a controller regarding a personal data breach indicating that a malicious third party had gained unauthorised access to the controller's systems. The LSA also received three follow-up notifications. The LSA was informed that the controller had discovered the breach on 21 October 2019 and had immediately engaged an external service provider to block the attacker and to prepare a forensic report analysing the affected systems and the personal data involved. According to the forensic analysis, the attacker had focussed on exploratory activities but had also copied network documentation, business and other documents, as well as six mailboxes to a remote location. The mailboxes had been found to contain files with personal data. On 25 February 2020, 81,000 data subjects (employees and customers of the controller) were notified of the breach. The personal data affected included first name, last name, date of birth, flight information, booking number, luggage information, as well as wheelchair requirements. For

(potential) employees, more data were affected, including, resumes and business contact information.

The LSA concluded that, at the time of the breach, the controller was processing personal data of over 25 million individuals. Of these, personal data of up to 83,000 individuals and health data of 367 individuals were leaked. According to the controller, 90% of the affected data subjects are Dutch, based on the point of sale. The controller could not provide a breakdown of other countries of origin but considering the amount of information, the LSA decided that 10% still amounts to data subjects from other EU countries being substantially affected.

The LSA investigated whether the technical measures taken by the controller with regard to access to personal data were appropriate as required by Art. 5(1)(f) GDPR in conjunction with Art. 32 GDPR. It was determined that the attacker had used a "password spray" or "credential stuffing" attack, i.e. applied, frequently used or previously leaked passwords. The cause of the breach was a simple and frequently used password that was easy to guess by automated means. The password strength and level were not in accordance with the authentication policy of the controller. Furthermore, the periodic security checks conducted by the controller had shown that the controller's password policy had not been adhered to. In addition, the LSA considered that dividing the controller's network into several segments could have prevented the attacker from gaining further access to the controller's systems and that users' privileges could have been better adjusted. Given the state of the art and the implementation costs, the LSA considered that the technical measures implemented at the time of the breach were not appropriate within the meaning of Art. 32 GDPR.

The LSA imposed on the controller an administrative fine of EUR 400,000 for the infringement of Art. 32(1) and (2) GDPR.

LSA: Spanish SA

Personal data breach / Hacker-attack / Data security / Administrative fines

Year of decision: 2021

OSS register number: EDPBI:ES:OSS:D:2021:239

The controller, a company owning a web platform, was hit by several cyber-attacks from an unidentified third party who accessed its database hosted on the platform of a cloud service provider. On 29 June 2018, the controller notified the LSA of a first cyber-attack, which occurred on 27 June 2018 and resulted in the unauthorised access to the personal data of 232,766 customers residing in more than 170 countries (comprising almost all EU member states). On 27 July 2018, the controller notified the LSA of a second data breach, which occurred on 25 July 2018, and resulted in the unauthorised access of the usernames and email addresses of 2,892,786 account holders. In response to these data breaches, the controller implemented several technical and organisational corrective measures.

Following the notification of the two data breaches, the LSA initiated investigations into a possible breach of Arts. 32, 33 and 34 GDPR. As a result of these investigations, the LSA found that the controller failed to implement up-to-date technical and organisational security measures, taking into account the degree of risk of the processing activities carried out. Considering that these security deficiencies were to a large extent responsible for the occurrence of the above-mentioned incidents, the LSA ruled that the company infringed Art. 32(1) GDPR. Nonetheless, the LSA pointed out that the company notified the breaches in accordance with its obligation under Art. 33 GDPR. Finally, in light of the evidence at hand, the LSA concluded that there was no high risk to the

rights and freedoms of natural persons that would require informing data subjects in accordance with Art. 34 GDPR.

The LSA imposed an administrative fine of EUR 100,000 on the controller for the infringement of Art. 32(1) GDPR.

LSA: French SA

Personal data breach / Data security / Passwords / Data subject rights / Administrative fines

Year of decision: 2021

OSS register number: EDPBI:FR:OSS:D:2021:181

Following the notification of a personal data breach on the controller's website affecting 210,692 European nationals, the LSA conducted both on-site and online audits of the controller to verify its compliance with the GDPR. Thereafter, the LSA also carried out a second on-site control in the context of the LSA's investigations regarding five complaints received from customers and prospects concerning the commercial prospecting by the controller they have been subject to, as well as the exercise of their rights.

The LSA found that the controller did not facilitate the exercise of data subject rights, as the email address provided to them for this purpose was defective. In addition, the LSA pointed out the complexity of the right of access procedure implemented by the controller for prospects receiving postal solicitations. Therefore, the LSA considered that the controller failed to comply with its obligations under Art. 12(2) GDPR.

Following its investigations regarding the data breach notification, the LSA found that the controller had failed to ensure the security of the personal data it processed. Firstly, the LSA found that the controller did not ensure the effectiveness of the technical and organisational measures implemented by its processor. In this regard, the LSA concluded that the controller should have been more vigilant in complying with security standards considering that it had already been sanctioned by the LSA for security issues involving the same processor. Finally, the LSA considered that the controller's requirements regarding the robustness of passwords, when it comes to their length and complexity, were insufficient to ensure the security of the personal data processed and to prevent third parties from accessing the personal data. The LSA recommended that a password have at least 12 characters - containing at least one capital letter, a lower-case letter, a digit and a special character - or at least eight characters - containing three of these four characters - if it is accompanied by an additional measure, such as the timing of access to the account after several failures, setting up a mechanism to guard against automated and intensive attempts and/or blocking the account after several unsuccessful authentication attempts. The LSA imposed an administrative fine of EUR 250,000 on the controller. In addition, the LSA imposed a compliance order on the controller to remedy its breaches of Art. 12 and Art. 32 GDPR with a penalty payment of EUR 500 per delayed day, starting from the end of a period of three months following the notification of the decision.

LSA: French SA

Transparency / Right to erasure / Data security / Passwords / Administrative fines

Year of decision: 2021

OSS register number: EDPBI:FR:OSS:D:2021:279

The LSA carried out a volition audit at the premises of a controller in order to verify its compliance with the GDPR. The audit focused on the processing of personal data relating to the company's current and prospective customers. More specifically, the LSA investigated the information provided to

data subjects, compliance concerning data subjects' rights and data retention periods. In order to complete these investigations, the LSA also carried out an online audit relating to all processing accessible from the controller's website, with a particular focus on, among other issues, the methods used for informing data subjects.

In the course of its investigation, the LSA noted that the active database of the controller contained personal data of 16.653 persons who had not placed an order in more than 5 years and 130,000 persons who have not signed into their customer account in more than 5 years. In this regard, the LSA ruled that, although the controller implemented a retention period policy, personal data were kept for much longer periods than those specified in this policy on the day of the audit and did not appear to be appropriate for the purposes for which the data were processed (Art. 5(1)(e) GDPR). Furthermore, following its on-site and online audits, the LSA found that certain mandatory information provided for by Art. 13 GDPR was missing, namely the contact details of the DPO, the data retention periods, the legal basis of the processing and information on certain data protection rights. Nonetheless, the LSA noted that the company had complied with all the points raised regarding the information of data subjects by the end of the investigation.

As to the controller's obligation to comply with requests to delete personal data (Art. 17 GDPR), the LSA found that when an individual requested the deletion of its account, the company simply deactivated the account in question. In this regard, the LSA stressed that the email address used for marketing purposes should have been deleted in the event of withdrawal of consent insofar as its retention is not legitimate on any other basis. The company took measures in the course of the procedure, but did not fully achieve compliance, so the LSA issued an injunction against the company.

Finally, the LSA found that the format of passwords when both creating an account on the controller's website and accessing the customer databases were insufficiently robust to ensure data security within the meaning of Art. 32 GDPR. The LSA found further infringements of the same provision due to the obsolete nature of the hash function used for the storage of passwords of employees using the controller's website and the use of the same account by several employees when accessing a copy of the controller's production database.

The LSA imposed an administrative fine of EUR 300,000 to the controller for breaching Art. 5(1)(e), Art. 13, Art. 17 and Art. 32 GDPR. In addition, the LSA imposed a compliance order on the controller to remedy its breach of Art. 5(1)(e) GDPR with a penalty payment of EUR 500 per delayed day, starting from the end of a period of three months following notification of the decision.

LSA: Lithuanian SA

Personal data breach / Data security / Publicly available data / Administrative fines

Year of decision: 2021

OSS register number: not available yet

The LSA started inspections on its own initiative upon receiving information that personal data of 111,052 customers of the controller (among which 433 residing in other EU countries), including personal identification numbers, had been made publicly available. The LSA subsequently received a data breach notification and additional information from the controller.

The case was opened on the basis of a motion for imposition of an administrative fine sent by the LSA to the controller on 25 May 2021. The motion established that the personal data made public had been received from the backup copy of a

database stored in the controller's online storage without protection. The unprotected database had been created on 27 February 2018, meaning that the breach had existed from this date until 16 February 2021 when the controller suspended external access to the database, hence the applicability of the GDPR to the case. The controller provided clarifications with regard to the motion, alleging procedural irregularities, including the unreasonable extension of the investigation, the improper definition of the GDPR applicability to the case and factual errors, all of which the LSA considered and responded to in its final decision.

Analysis of the data stored in the database showed that personal data (names, driving licences, payment cards) had been stored in open text without encryption, and the passwords in the database encrypted with SHA-1 had been weak and unsafe. The controller had failed to purchase additional log record services for the database making it difficult to determine when and how many times customer data had been misappropriated. Considering this, the LSA found that the controller had performed post-breach security analysis (audits of firewalls, access rights, testing systems etc.) and had complied with Art. 33(3) GDPR. However, the LSA established that by failing to ensure proper access control and restrictions, by enabling third parties to access the file containing personal data without authorisation, by failing to ensure confidentiality of data stored in such file, by failing to record and store log records of access to and actions with the file, the controller had failed to comply with the requirements of Art. 32(1)(a) and (b) GDPR.

In addition, by failing to ensure proper management and control of the security of personal data, to appoint a competent person responsible for security and risk management, to segregate the duties and limits of responsibilities in the area of IT creation and maintenance from those in the area of cyber security, and to ensure recording, monitoring and assessment of access to and actions with the file, the controller had violated the requirements of Art. 24(1) and Art. 32(1)(d) GDPR. As a result, the breach had created a risk to the rights and freedoms of natural persons, such as possible identity fraud, unlawful tracking, social engineering and others.

In light of the above, the LSA imposed on the controller an administrative fine of EUR 110,000 for breach of Art. 32(1)(a), (b) and (d) GDPR.

6.1.3.2. Selection of other cases on the interpretation of GDPR provisions

LSA: Latvian SA

Special categories of data / Biometrics / Fingerprints / Lawfulness of processing

Year of decision: 2021

OSS register number: not available yet

The LSA received information that a sports club is processing data subjects' (clients) fingerprints for customer identification in order to permit clients to enter the premises of the sports club. After investigating the circumstances of the incident, the LSA established that the controller used a biometric access control system in order to provide access control of clients to the sports club's premises. The LSA established that biometric data uniquely identifying natural persons were processed without a GDPR compliant legal basis and in disregard of the GDPR in regard to the principles of processing personal data. From 2016 until 2021, the controller processed biometric data of approximately 3,000 data subjects in order to ensure access control to the premises.

The LSA imposed an administrative fine of EUR 5,836 on the controller. The LSA also ordered the controller to delete the biometric data of clients (both existing and former), including a digital fingerprint point card created from a fingerprint

and to comply with the requirements of the GDPR. When imposing a fine, the LSA took into account the nature of the incident, the duration, the importance and purpose of the processing, the number of persons concerned, the conduct of the controller with a view to mitigating the damage suffered by the data subjects (the controller, following the LSA's request, ceased the processing of personal data), as well as the fact that the controller ensured cooperation with the LSA during the investigation.

LSA: Cypriot SA

Special categories of data / Health data / Employment / Lawfulness of processing / Consent / Data minimisation

Year of decision: 2021

OSS register number: EDPBI:CY:OSS:D:2021:175

The LSA investigated a complaint against the controller whose main activity is the provision of recruitment and placement services for cruise ships. Prior to starting work on a ship, the controller requests from employees to sign a general authorisation for the release of medical records in order to have access over them and be able to assist the employees with medical care, to arrange any associated travel and to handle any medical claim, in the event of a medical incident taking place on-board.

The LSA found that the authorisation appears to be based on the consent of the employee. However, the LSA considered that the condition of freely given consent was not fulfilled in the present case, as employees of the controller who are requested to sign the privacy notice in advance upon commencement of employment, had no real choice. Consequently, consent is not considered to be freely given when the employee is unable to refuse or withdraw his or her consent without detriment. The LSA recalled that in line with Art. 7(3) GDPR, the data subject shall have the right to withdraw their consent at any time and the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The LSA also considered that in the employment sector, in general, consent should not be used as the lawful basis for the processing due to the imbalance of the relationship between employer and employee. The LSA further stated that in line with the principle of data minimisation the controller should collect and generally process only data that are absolutely necessary to be able to assist the employees. The LSA was called upon to assess whether the controller could rely on another legal basis for the collection and general processing of employees' health-related data, other than consent. The LSA explained that the controller could possibly rely on Art. 9(2) GDPR, as it provides a list of possible exemptions to the ban on processing special categories of data, if certain additional conditions are fulfilled by the controller.

The LSA ordered the controller to cease the processing of health data of employees based on consent, to bring the processing into compliance with the provisions of the GDPR and in particular to take actions that consist of processing only the health-related data in the employment context which are necessary for the discharge of obligations laid down by law or by the collective agreements for the purposes of the recruitment, the performance of the contract of employment, health and safety at work, and the exercise and enjoyment of the rights and benefits of employees, as well as to inform the LSA on the actions taken to comply with its decision at the latest within one month from the date of the decision.

LSA: Swedish SA

Right to erasure / Legitimate interest / Payment data / Transparency and information

Year of decision: 2021

OSS register number: EDPBI:SE:OSS:D:2021:196

This case before the Swedish SA involved a complainant who previously had an account and a payment subscription to the controller's services. The complainant requested several times for his card details to be erased by the controller. According to the controller, it only processes unique identifiers for the payment cards or "instruments" (unique payment instrument identifiers) used by a customer when registering for free trial periods. The legal basis for the processing is legitimate interest. The controller considered that the continued processing of the data is not subject to the right to erasure because the controller has a strong, legitimate interest in continuing the processing that outweighs the rights and freedoms of the complainant, as the processing is necessary for the controller in counteracting fraud.

The LSA recalled that for processing to be based on Art. 6(1)(f) GDPR, all three conditions provided therein must be fulfilled. Firstly, the controller or third party has a legitimate interest (legitimate interest), secondly, the processing is necessary for purposes of legitimate interest (necessary) and third the interests or fundamental rights and freedoms of the data subject do not weigh heavier and require the protection of personal data (balance of interest). The LSA analysed the three conditions and in light of the reasons the controller had presented, the LSA found that the controller demonstrated compelling legitimate grounds that outweigh the complainant's interests, freedoms and rights. The controller thus had the right to continue processing the data after the complaint objected to the processing and the complainant was therefore not entitled to erasure under Art. 17(1)(c) GDPR.

Nevertheless, the LSA concluded that the controller's response to the complainant had not been sufficiently justified pursuant to Art. 12(4) GDPR because the controller had not clearly stated what personal data is being processed, that the data is processed on the basis of a legitimate interest and what the legitimate interest is and that the answer did not contain information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. The controller had thus processed personal data in violation of Art. 12(4) GDPR.

The LSA issued a reprimand to the controller.

LSA: French SA

Data subject rights / Data retention / Data security / Data processing agreements / Record of processing activities

Year of decision: 2021

OSS register number: EDPBI:FR:OSS:D:2021:202

This case involved a controller who runs a platform for rental vehicles, which puts vehicle owners in contact with private individuals. One of the controller's customers complained that his driving license was accessible via any browser with no authentication required, by entering an URL that connected to a software tool of the controller's subcontractor. The complainant stated that he had made several requests for deletion of his driving license but to no avail.

Upon investigation, the LSA found that although the controller had defined a policy on data retention periods, in practice there had been no restriction on the retention of data relating to the creation of users' accounts. According to the LSA, this constituted a breach of the obligations of Art. 5(1)(e) GDPR.

Furthermore, the LSA found that customer records created by the controller were not anonymised and it was still technically possible to re-identify customers from their user numbers by, for example, cross-referencing them with other indirectly identifying personal data. Therefore, the general data erasure procedure implemented by the controller did not guarantee data subjects' right to erasure and the controller breached Art. 17 GDPR.

The controller had entrusted verification of the identities of its users' profiles to two service providers processing personal data on its behalf. However, the relevant service provision contracts did not satisfy the requirements of Art. 28(3) GDPR. In addition, according to the LSA, although the controller had fewer than 250 employees, it was carrying out a variety of personal data processing operations regarding prospects and customers on a regular basis and for purposes such as marketing, customer management and combating fraud. Despite that, the controller did not keep a record of processing activities and breached Art. 30 GDPR. Finally, the controller did not implement appropriate security measures to protect from potential unauthorised access to the supporting documents sent by users via email and retained the passwords to over 150,000 user accounts in a form that did not ensure their confidentiality. The LSA also found that the way of communicating data in response to access requests was exposing the data to a risk of compromise in the event of an attacker's intrusion into the data subject's inbox or interception of emails by an unauthorised third party.

The LSA ordered the controller to comply with the above-mentioned GDPR provisions and to adopt, within three months, the following measures: define and implement a policy on retention periods for its customers' and prospects' data, define and implement an effective procedure for the right to erasure, complete the contracts with the data processors by including the missing terms, keep a record of processing activities, take all necessary security measures, so as to ensure the security of the data and prevent unauthorised third parties from accessing them.

LSA: Icelandic SA

Personal data breach / Data security / Education

Year of decision: 2021

OSS register number: EDPBI:IS:OSS:D:2021:216

This case of the Icelandic SA involved a controller which is a company developing and operating an online information system intended for schools and other entities working with children, which allows for information exchanges between schools and parents. The case was opened after the controller informed the LSA via telephone of a data breach that had occurred in February 2019 due to a vulnerability within the online information system. The breach was made on purpose, by one of the students' parents, who wanted to expose faulty security within the system. The parent was able to access data from 423 students in 90 schools in Iceland while logged in, by using a script creating a random number in the visible web page address number found in the URL-bar (address-bar) of each student's personal page. Students' names and profile pictures and in some instances national identification numbers of students and/or their custodians were disclosed. The parent also contacted another person with access to the same system in Sweden who was able to access the national identification number and avatar of one child in Sweden.

The controller stated that, immediately after becoming aware of the breach, it had activated an action plan and had informed the principals of every elementary school in Iceland. The LSA carried out an investigation and found, on the basis of the information and data provided by the controller, that human error led to the data breach since a solution for the vulnerability, which had already been created, had not been fully implemented. Insufficient follow-up and

testing of security measures then led to this fact not being discovered until after the data breach had already occurred. The LSA concluded that the controller did not comply with the requirements of Art. 32(1)(b) and (d) GDPR, Art. 5(1)(f) GDPR and the relevant national law provisions.

Additionally, the controller did not ensure proper security of personal data of the data subjects affected by the data breach, because it had mistakenly sent national identification numbers to the wrong schools and data protection officers and therefore did not comply with Art. 5(1)(f) GDPR and relevant national law provisions.

The LSA imposed an administrative fine of ISK 3,500,000 (approximately EUR 238,475) on the controller.

LSA: Berlin SA

Right to erasure / Lawfulness of processing

Year of decision: 2021

OSS register number: EDPBI:DEBE:OSS:D:2021:229

On 29 April 2018, a complainant requested the controller to erase his personal data and to close his customer account. The controller confirmed to the complainant the erasure by an email on 30 April 2018. In spite of this confirmation, the complainant submitted that a few months later he received an email from the controller informing him that the email address of his customer account had been changed. The complainant contacted the controller again, insisting that his customer account should have been erased. The account was finally erased on 26 March 2019.

In the course of its communication with the LSA, the controller explained its procedure applicable to requests for erasure and stated that the delay in the current case could have been due to obstacles, which were no longer possible to assess. In addition, the controller claimed that the alleged violation should have been assessed in light of the national law applicable prior to the GDPR's entry into application.

The LSA first explained that although the failure to erase the complainant's personal data is a processing that started before the 25 May 2018, the GDPR applies because the complainant's request was not complied with until 26 March 2019. Therefore, the lawfulness of the processing of personal data has to be assessed in light of the GDPR.

The LSA found that the failure to erase the complainant's customer account constituted a violation of Art. 17(1)(a) and (b) GDPR, in conjunction with Art. 6(1) and Art. 5(1) GDPR. It recalled that if one of the grounds listed in Art. 17(1) GDPR applies, the controller has to erase the complainant's data immediately, i.e. without undue delay. The LSA also found that the controller could not successfully invoke any of the exceptions under Art. 17(3)(e) GDPR.

First, regarding the violation of Art. 17(1) GDPR, the LSA concluded that with the declaration of the request for erasure on 29 April 2018, the purpose of processing had ceased to exist and erasure was possible on the basis of Art. 17(1)(a) GDPR. By requesting the closure of his customer account, the complainant had initiated the end of the customer relationship, so continued storage of the data was no longer necessary within the meaning of Art. 6(1)(b) GDPR. In addition, according to the LSA, the data subject was entitled to request deletion of his personal data based on Art. 17(1)(b) GDPR too, since the request for erasure implicitly includes the withdrawal of consent within the meaning of Art. 7(3) GDPR. The retention of the personal data could not be based on Art. 6(1)(f) GDPR, as there was no overriding legitimate interest in not erasing the data and there were no actual indications for the existence of grounds for obstruction (e.g., outstanding invoices). Moreover, the controller could not successfully invoke any of the exceptions under Art. 17(3) GDPR.

Second, the LSA concluded that continued storage of the complainant's personal data also constituted a violation of Art. 6(1) GDPR because there was no legal basis for the continued storage of the data after the request for erasure. The controller bears the burden of proof for the existence of one of the conditions mentioned in Art. 6(1)(a) to (f) GDPR, which was not provided in the present case.

In light of the above, and since it could not be clearly established whether the e-mail address of the customer account had been changed before the request for erasure, the LSA issued a reprimand to the controller.

LSA: Spanish SA

E-commerce / Transparency / Lawfulness of processing / Data subject rights / Right to be informed / Right to object

Year of decision: 2021

OSS register number: EDPBI:ES:OSS:D:2021:263

Following a data subject's complaint launched in Germany, the LSA found that the privacy policy of the controller's website was difficult to read due to a large number of grammatical and spelling errors, and that its structure was confusing. As a result, the LSA found that the privacy policy violated Art. 12(1) GDPR regarding the obligation to provide information to data subjects in a concise, transparent, intelligible and easily accessible form. Additionally, several shortcomings were identified by the LSA as to the content of the controller's privacy policy, resulting in a violation of Art. 13 GDPR.

In particular, the LSA ruled that the information concerning the right to object under Art. 21(1) GDPR is drafted in a confusing manner which made it more difficult for data subjects to exercise their right to object to processing of their data for direct marketing purposes. As a result, an infringement of Art. 21(4) GDPR was found by the LSA. Finally, the LSA considered that, as the complainant had the right to request a simplified invoice without being asked for an identification number to be issued, the controller infringed Art. 6(1) GDPR and, consequently, the principle laid down in Art. 5(1)(a) GDPR.

In view of the above, the LSA imposed on the controller an administrative fine of EUR 6,000 for infringements of Art. 5(1)(c), Art. 6(1), Art. 12, Art. 13 and Art. 21 GDPR. The controller was given three months to align its privacy policy with Arts. 12 and 13 GDPR, as well as to stop requesting the customer's tax identification number, unless it obtained valid consent or it is required by law to process this data.

LSA: Romanian SA

Data subject rights / Right to erasure / Right to be informed / Publicly available data

Year of decision: 2021

OSS register number: not available yet

The investigation started following a complaint from a Polish citizen claiming that their personal data had been published on the website of the controller without their consent and that they had requested data erasure. The controller, headquartered in Romania, manages online catalogues based on data collected from public databases from various countries in order to facilitate the fast search of information related to over 60 million companies and professionals. The website is available in various versions of European domain names and in the national languages of multiple EU Member States.

According to the controller, the identification elements of the complainant in the controller's online catalogue included the professional name and address, the trade register number, the fiscal attribute and the field of activity, which were all collected from a public database. The controller also indicated

that the deletion option was accessible on the website without the controller being notified. The controller further explained that the complainant's request on the website had not been processed by error and their subsequent email had been sent to spam and not processed on time. Consequently, the controller found out about the request only after the LSA contacted them and immediately took measures to erase the data and inform the complainant.

The LSA found that the controller did not handle the request in accordance with Art. 17 GDPR and did not send a reply within the deadlines provided by Art. 12(3) GDPR. The LSA also recalled that, pursuant to Art. 24 GDPR, the controller is obliged to implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the GDPR. This includes appropriate and effective measures guaranteeing that all requests received via publicly provided contact details are assessed and handled under the conditions and deadlines provided for in Art. 12 to Art. 22 GDPR.

Furthermore, the LSA concluded that the controller had not provided the data subject with the complete information required under Art. 12 to Art. 14 GDPR, including information regarding the legal basis of the processing. The LSA highlighted that all situations, in which a controller processes information allowing the identification of individuals, even if related to their professional activity, fall within the material scope of the GDPR.

In light of the above, the LSA issued reprimands to the controller. The LSA also imposed corrective measures on the controller: to implement appropriate technical and organisational measures, including appropriate data protection policies; to ensure the lawfulness of the processing in accordance with Arts. 5 and 6 GDPR of personal data that is available in online catalogues; to provide all the necessary information in accordance with Art. 12 to Art. 14 GDPR and to ensure respect of the data subjects rights, as provided by Art. 15 to Art. 22 GDPR.

LSA: Maltese SA

Restriction of processing / Data subject rights / Debt collection

Year of decision: 2021

OSS register number: EDPBI:MT:OSS:D:2021:272

In this case, a complainant alleged that the controller obtained his personal data from an unspecified source and was requesting repayment of a loan which the complainant never took. The complainant also stated that he had been a victim of identity theft by a third party and requested to determine how his data had come into the possession of the controller.

In response, the controller stated that it had been informed by the police about the illegal use of the complaint's personal data and had immediately stopped all debt collection activities. The controller had also received a letter from the complainant requiring refraining from processing any personal data of the complainant and to discontinue any communication with regard to the loan. The controller had decided not to reply to this letter based on the understanding that any further communication was undesirable for the complainant. As to the source, from which the personal data had been collected, the controller explained that it had been obtained through a loan application via the website after the applicant's identity had been verified. The controller also informed the LSA that it was subject to legal obligations under which the retention period for personal data related to loan applications and agreements could be up to 10 years.

On the question of determining the source of the complainant's personal data, the LSA noted that the complainant had not

explicitly asked the controller to provide him with information regarding the source of his data. Nevertheless, the controller did provide this information to the LSA. As regards the request to restrict the processing of the complainant's personal data, the LSA found that the controller acknowledged and complied with the complainant's request to restrict the processing of his personal data. Regarding the lack of response by the controller, the LSA noted that the controller violated Art. 12(3) GDPR which lays down an obligation to provide the complainant with information on the action taken on a request under Art. 15 to Art. 22 GDPR, without undue delay and in any event within one month of receipt of the request. As regards the request for erasure, the LSA agreed that the data could not be deleted because processing was necessary to comply with national legislation to which the controller is subject.

The LSA issued a reprimand to the controller.

LSA: Norwegian SA

Lawfulness of processing / Performance of contract / Direct marketing / Right to object

Year of decision: 2021

OSS register number: EDPBI:NO:OSS:D:2021:292

This case involves a complainant who hadbeen receiving direct marketing by email without having the possibility to opt out upon registration of his email address. He had objected to this processing in September 2018, yet he still received a direct marketing email in November 2019. The complainant contacted the DPO of the controller on several occasions, and at times, his requests were answered in more than one month. When he requested the legal basis for the processing of his personal data, which he believed to be consent under Art. 6(1)(a) GDPR, the DPO wrote in response that the legal basis was rather a necessity for the performance of a contract pursuant to Art. 6(1)(b) GDPR. Later, in another email to the complainant, the DPO stated that the legal basis was Art. 6(1)(f) GDPR for the purpose of marketing the controller's similar products and Art. 6(1)(b) GDPR for the purpose of marketing in relation to the customer benefit program.

The LSA established that there was no designated opt out possibility for marketing from the controller, but it was possible to 'approve' digital marketing via email and SMS on the user's page. As regards the lawfulness of the processing, the LSA reasoned that processing based on contractual performance must be objectively necessary, i.e. the controller should be able to demonstrate how the main subject matter of the specific contract with the data subject cannot be performed without the specific processing of the personal data in question. The processing of personal data for marketing purposes by the controller was not necessary for the performance of the contract related to the provision of a credit card service, and therefore, Art. 6(1)(b) GDPR could not provide the legal basis for the processing. The LSA found that the controller could not retroactively change the legal basis (from contractual performance to legitimate interest) after having commenced with the processing, as this leads to a lack of predictability for the data subject. In any event, a change in the legal basis for processing shall be communicated to the data subjects pursuant to Art. 12 to Art. 14 GDPR.

Further, the LSA found that the controller breached Art. 21(3) GDPR by continuing the processing of the complainant's personal data for direct marketing purposes after his objection to the controller's DPO. The provision of insufficient information on the legal basis of processing and the failure to inform the data subject on his right to object to processing for direct marketing by the controller constituted a breach of Art. 13(1), Art. 12(1) and Art. 21(4) GDPR. Finally, the controller's delays of over a month to respond to the complainant's requests, and without giving him reasons for these delays, constituted a breach of Art. 12(3) GDPR.

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

LSA: Swedish SA

Join controllership / Direct marketing

Year of decision: 2021

OSS register number: EDPBI:SE:OSS:D:2021:236

A complainant stated that a company provided the complainant's email address to a third party for the purpose of sending direct marketing to the complainant without having a legal basis for it. In December 2018, the complainant requested from the third-party access to his data under Art. 15 GDPR, which revealed that the company disclosed the complainant's personal data to the third party. The company stated that this took place in 2017, before the introduction of the GDPR on 25 May 2018 and as such, in 2017, when the complainant's email address was sent to the third party in order to be able to target marketing using the third party's custom audience function. This process was carried out in accordance with the applicable legislation.

In spring 2018, before the introduction of the GDPR on 25 May 2018, the third party changed its terms for the custom audience function and placed the data in quarantine until the company would accept the new terms and conditions of the third party. During this period, the company did not have access to or the possibility to use, modify or delete the personal data. The company approved the third party's new terms in January 2019 and the quarantine personal data was then unlocked by the third party, after which the company deleted the complainant's information.

According to the company, it was only the controller for the transfer of the complainant's personal data to the third party and for any direct marketing that took place before the personal data was quarantined, i.e. before the GDPR began to apply. Furthermore, the company stated that during the period of the GDPR, the company only processed the data subjects' personal data for direct marketing with their prior consent.

The LSA examined whether the company has been a joint controller during the time the personal data was quarantined, i.e. from spring 2018 (before the introduction of the GDPR and when the controller did not approve the third party's conditional changes) until January 2019 (when the personal data was erased). The LSA found that the company transferred the complainant's email address to the third party for the purpose of direct marketing to the complainant. From the moment the personal data was locked by the third party, no direct marketing has been made to the complainant. Since the company did not approve the third party's conditional amendments, it could not continue to process the personal data for the purpose it was transferred to the third party. The company also did not instruct the third party to store the personal data in quarantine. In these circumstances, the purpose of the processing seems to have changed when the third party unilaterally decided to quarantine the complainant's personal data. This indicates that the third party alone determined the purpose and means of processing and that the third party has been solely responsible for the continued processing (storage).

According to the LSA, in this case, it has not been shown that the company had the opportunity to dispose of the data or affect the processing of the data while quarantined. Furthermore, the company has stated that it lacked knowledge of whether the third party has directed direct marketing to the complainant while the personal data was locked. In an overall assessment of the circumstances, the LSA found that

the company cannot be regarded as a joint data controller while the personal data was locked by the third party.

This supervision covers only the company's processing of the complainant's personal data in accordance with the GDPR. The LSA, therefore, found that the investigation in the case did not show that the controller had processed the complainant's personal data in violation of the GDPR. The LSA decided to close the case.

6.1.4. Mutual assistance

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

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

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

Between 1 January 2021 and 31 December 2021, SAs initiated 243 formal mutual assistance procedures and 2418 voluntary mutual assistance procedures.

6.1.5. Joint operations

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

In 2021, SAs did not carry out any joint operation.

6.2. NATIONAL CASES

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

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

6.2.1. Some relevant national cases with exercise of corrective powers

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

Several cases highlighted a lack of proper technical and organisational measures for processing personal data securely, which led to data breaches. Many other cases revolved around data processing without a data subject's consent. Some significant incidents involved the unlawful processing of special categories of personal data, such as health data. Numerous cases involved data subjects who could not effectively exercise their rights, such as the right of access, the right to erasure and the right to object to a processing act. A great number of cases also include the controller's failure to notify the data subjects of the occurred or the potential risk of data breaches. The entities fined were from both the private and the public sectors.

6.2.1.1. Austria

The Austrian SA carried out several investigations and gave a number of fines and warnings during 2021.

On 17 February, the Austrian SA imposed a fine of EUR 4,000,000 on an Austrian bank for failing to ensure that the bank customer data processed as part of an Excel file, which had been unintentionally sent to 227 unauthorised recipients, was encrypted or otherwise protected by an access authorization system that would prevent unauthorised access and unintentional disclosure to third parties.

On 26 July, the Austrian SA issued a fine of EUR 2,000,000 on a data controller that processed data, for a loyalty program, solely based on invalid consent. In particular, it found that the requests for consent from the data controller were designed in such a misleading manner that no valid consent by the data subjects could be assumed. This made the data profiling unlawful, retrospectively for the entire period.

On 28 September, the Österreichische Post was fined EUR 9,500,000 for failing to facilitate the exercise of data subjects' rights. In fact, the controller systematically restricted their rights by ignoring and not processing inquiries sent by email, which were later disposed of together with the mailbox. The affected data subject had to submit a completely new application through a predefined contact form, regardless of their previously submitted inquiry through email. The contact form also limited the ways in which the data subjects could identify themselves.

6.2.1.2. Belgium

The Belgian SA addressed numerous complaints and found violations by data controllers on issues related to, among others, transparency, data subjects' rights, marketing, trading data, smart cameras and COVID-19. This section expands upon a selection of interesting cases.

In January, the Litigation Chamber of the Belgian SA issued a fine of EUR 50,000 and ordered the controller, a company distributing promotional packages, to comply with the GDPR. The decision was made in consideration of the number of data subjects affected, the seriousness of the breach and the nature of the data processed. In particular, it found that the controller did not properly inform the data subjects about the trading of their data and the consent given by them for these data transfers were not valid, as consent was clearly not informed, but also not specific or freely given.

Later in April, the Belgian SA adopted a decision on the responsibility of a controller (a bank) for the abusive usage of the IT system by one of its employees. The controller was fined EUR 100,000 and was ordered to make all employees' access to the database of the Central Individual Credit Register of the Belgian National Bank compliant with Art. 5(1)(f) and Art. 32 GDPR. To achieve such compliance in a transparent and traceable manner, the controller should keep a journal of IT logs.

In December, there were four cases worth highlighting.

The first one revolves around a controller who was sanctioned for not complying with a request to erase personal data in the context of unsolicited direct marketing communication. The Litigation Chamber of the Belgian SA established that the controller's actions amounted to a violation of Art. 12, Art. 14, Art. 15, Art. 17 and Art. 21 GDPR. In addition, it ordered the controller to inform, within 1 month, all data subjects whose personal data had been acquired and further issued a fine of EUR 10,000.

The second case concerned the exercise of the right to be forgotten. A press group refused to delete numerous press articles archived and available on their website that contained personal data of the complainant. Despite the complainant's efforts in arguing for deletion, anonymisation or replacement of his identity with his initials, the Belgian SA dismissed the complaint by indicating that the press publishers were right to refuse the requested deletion.

In the third case, a reprimand was issued against the petition platform Change.org (the controller) for repetitively sending emails. The controller was ordered to communicate, at the first moment of contact with the email recipient, how can the data subjects' rights be exercised more transparently, but also include a link to its privacy policy. In order, to ensure compliance, the controller was ordered to submit evidence of compliance to the Belgian SA.

The fourth case concerned a controller's IT system that did not permit the full enjoyment of the right of correction and also dealt with an issue of conflict of interest of the controller's DPO. The Belgian SA discontinued the proceedings for infringement of Art. 5(1)(d), Art. 16 and Art. 25 GDPR since the controller (a bank) proved that the necessary steps were taken to process the diacritical marks in the names of the clients. However, as the conflict of interest on the part of the bank's DPO constituted a violation of Art. 38(6) GDPR, the controller was issued a fine of EUR 75,000.

In 2021, the Litigation Chamber of the Belgian SA also handled another interesting case in relation to smart cameras and the use of cookies. It was concluded that there was no infringement pertaining to the setting up of cameras by the controller Westtoer at the Belgian coast to measure the number of visitors during the summer months due to the risks associated with COVID-19. However, the Litigation Chamber reprimanded the controller and ordered to bring certain things (such as the consent for the use of cookies on Westtoer's website, its register of processing activities and its privacy policy) into compliance.

6.2.1.3. Bulgaria

In 2021, the Bulgarian SA experienced a continued increase in the number of complaints and actions taken from 2020. Up until 30 September, it issued a total of 408 decisions that addressed complaints from a number of different data subjects and legal entities, state authorities and organizations. Upon reviewing the complaints, the following corrective powers were imposed: one warning, 10 official warnings, three orders for execution of requests of a data subject and 66 orders for administrative penalties. Most violations were made by data controllers processing personal data in the area of courier services, heat accounting, hospitals and other medical institutions, as well as mass video surveillance. This section will cover a selection of cases.

The Bulgarian SA handled a case concerning illegal dissemination of personal data. It concluded a violation of Art. 32(1)(b) GDPR on the side of the controller, the Ministry of Health of the Republic of Bulgaria, and the processor, the liquidator of SBDPLFZR – Raduntsi. The SA issued two penal decrees imposing a "property sanction" on the Ministry of Health in his capacity as personal data controller and a

"penalty" on the liquidator in his capacity as personal data processor.

A public figure filed a complaint to the Bulgarian SA for the improper disclosure of personal information by the controller, a press media website, in a website article. The controller argued that the data had been processed for journalistic purposes. Bearing in mind the public nature of the data subject's profile, the case required a good balance between the right to protection of privacy and the right to freedom of expression and the right to information. The SA concluded that the publication of the complainant's date of birth and the full address was not in line with the principle of data minimisation, therefore that information needed to be deleted. Due to the violation of Art. 5(1)(c) GDPR, the SA issued a fine of EUR 2,500 on the controller. The decision of the Bulgarian SA was appealed twice, but the Supreme Administrative Court of Bulgaria finally confirmed and upheld the decision made by the SA.

A complaint has been raised before the Bulgarian SA against the Supreme Administrative Court of Bulgaria after denying a data subject's access to their assessed written work, which violated Art. 15 GDPR. Furthermore, upon a revision of the controller's internal rules and the register of processing activities, the SA established that the controller has managed to limit the scope of the concept of personal data.

6.2.1.4. Cyprus

The Cyprus SA issued multiple fines in 2021. The Cyprus SA carried out these enforcement acts:

- Issued a fine of EUR 925,000 on the controller WS WiSpear Systems Ltd for the collection and storage of Mac Addresses (Media Access Control Address) and IMSIs (International Mobile Subscriber Identity), in breach of GDPR Art. 5(1)(a) GDPR;
- Imposed a fine of EUR 40,000 on the controller APOEL FOOTBALL (PUBLIC) LTD for violating Art. 24(1) and Art. 32(1) GDPR and ordered it to inform potentially affected football fans by the data breach. The SA also issued another fine of EUR 40,000 on the controller OMONOIA FOOTBALL LTD for the violation of Art. 24(1) and Art. 32(1) GDPR and a fine of EUR 25,000 on the processor Hellenic Technical Enterprises Ltd for breaching Art. 28(1) and Art. 32(1) GDPR;
- Issued a EUR 10,000 fine to the Mediterranean Hospital of Cyprus for violation of Art. 31 and Art. 58(1)(a) GDPR due to its disregard of the SA Commissioner's orders and for avoiding cooperation with the SA.

The Cyprus SA also issued six fines to various controllers for providing unsolicited communication to data subjects, including the following:

- A fine of EUR 12,000 to the Democratic Party;
- A EUR 4,500 fine to the EDEK Social Democrats political movement;

6.2.1.5. Czech Republic

In 2020, the Czech SA fined a controller CZK 50,000 (EUR 2,000) for publishing personal data of participants in court hearings that were meant to be public in a limited time period. The SA stated that the controller did not have any legal ground to publish the data and highlighted that the right to privacy overrode interest in further data disclosure without considering the individuality of every case. The controller was further ordered to cease the processing of the personal data in a separate proceeding.

6.2.1.6. Denmark

Unlike in other EEA jurisdictions where the SAs have the authority to issue administrative fines themselves, in Denmark, the Danish SA first investigates a data protection

legal violation and then reports it to the police. The police then investigate whether there are grounds for raising a charge and finally a court decides on a possible fine.

In January, the Danish SA decided that the IT University of Copenhagen did not breach any data protection rules by using a supervision program for online exams. Later in February, the Danish SA handled a case where it decided that the controller Medical Services was not breaching any rules by recording telephone conversations, but it should have not kept the recordings for too long. The controller was ordered to delete all recordings that are more than five years old.

In March, the controller Statens Serum Institut (SSI) was sanctioned with serious criticism for its COVID-19 modelling project. In particular, the Danish SA critiqued SSI for initiating the processing of personal data without adequate risk assessment, impact assessment, consultation with the Danish SA, data processor agreements and appropriate safety measures.

In June, the Danish SA reported Nordbornholms Byggeforretning ApS to the police and recommended a fine of approximately EUR 54,000 due to the controller's unlawful disclosure of information about criminal offences of a former employee. In July, the Danish SA reported Medicals Nordic I/S to the police and proposed a fine of approximately EUR 80,000 for treating confidential and health information about citizens in connection with COVID-19 tests, without establishing the necessary security for the processing of the data. Additionally, upon investigation, it was assessed that the infringements were committed intentionally since the controller had not carried out the necessary risk assessments in connection with the processing.

In August, the Danish SA reported the Danish Immigration Service to the police and proposed a fine of approximately EUR 20,000 for failing to meet the requirements for an adequate level of security as per the GDPR.

In September, the Danish SA expressed serious criticism against the municipality of Helsingør for its processing of personal data that used a complex technology in which the data subjects were children and youth, with parts of the processing showing a lack of legal basis. Moreover, the municipality could not demonstrate possession of necessary documentation related to the processing, nor took any adequate organisational and technical measures to ensure the necessary level of security. In the same month, the SA reported Kræftens Bekæmpelse to the police and recommended a fine of approximately EUR 108,000 for the repeated problems with insufficient protection of health data of, among others, cancer patients' health information.

6.2.1.7. Estonia

On 30 July, the Estonian SA issued a precept with a penalty payment of EUR 20,000 (per point previously set out) on the controller Register OÜ. It requested the controller to terminate the processing of the data of natural persons on two websites until it meets the necessary data protection requirements.

On 5 August, the Estonian SA issued a reprimand to AS A&P Mets for the unlawful data processing which constituted a violation of the requirements of the GDPR and the Electronic Communications Act. The SA further noted that if the unlawful data processing continues, the SA has the possibility to consider imposing a penalty payment as previously indicated to the controller.

6.2.1.8. Finland

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

The Finnish SA handled a case concerning data protection violations connected to parking control fees. The SA issued a reprimand to the controller ParkkiPate for processing personal data in violation of the GDPR and ordered it to act in compliance with the law. In addition, the controller was issued a fine of EUR 75,000 by the sanctions board.

On the basis of GDPR infringements, the SA's sanctions board imposed a fine of EUR 8,500 on a controller for carrying out direct marketing with robocalls without the consent of the call recipients. The Finnish SA decided to permanently prohibit the controller from processing the personal data, gathered based on unlawful consent, for direct marketing.

The sanctions board of the Finnish SA issued a fine of EUR 25,000 on the controller for data protection violations connected to the processing of location data of employees. The employees doing remote work were required to record their working hours in a mobile application that required allowing the use of location data. The SA issued a processing ban on the controller, covering all processing related to location data being or having been collected with the application.

The Finnish SA reprimanded the National Police Board for illegal processing of special categories of personal data with facial recognition software (Clearview AI). Apart from the reprimand, the National Police Board was ordered to notify the data subjects of the personal data breach insofar as their identity could be determined, but to also request from the Clearview AI service the erasure of the data transmitted by the police from its storage platforms.

6.2.1.9. France

France handled a number of cases in 2021 where it issued significantly large fines. A selection of cases is presented in this section.On 11 January, the restricted committee of the French SA imposed a fine of EUR 75,000 on the controller, a company specialized in the development of IT solutions for independent food retailers. The French SA noted the controller's inadequacy in taking actions considering the increase of website attacks and the lack of implementation of intermediate measures that could have limited the risk of new data breaches. The SA further emphasised the ineffectiveness of the developed anti-robot tool and observed the possibility that all user accounts were exposed to attacks over a long period of time.

On 20 July, the controller SGAM AG2R LA MONDIALE was fined EUR 1,750,000 for processing operations that violated Art. 5(1)(e), Art. 13 and Art. 14 GDPR. The controller was in breach of Art. 5(1)(e) GDPR since it had not implemented the data retention periods it had defined. The violation of Arts. 13 and 14 GDPR was established based on the non-disclosure of the information regarding the recording of telephone calls and the right to object to being recorded. In addition, the lack of provided information of other data subjects' rights did not allow access to more comprehensive information.

On 26 July, the French SA's restricted committee imposed a fine of EUR 400,000 on MONSANTO for the disregard of its obligations under Art. 14 GDPR in terms of information and Art. 28 GDPR in terms of a contractual framework with a processor. In relation to Art. 14 GDPR, the French SA considered that the creation of contact files by lobbyists for lobbying purposes is not, in itself, illegal. However, the individuals who were listed on such file should have been informed of the existence of the file and consequently, allowed to exercise their right to object to such listing. With respect to Art. 28 GDPR, MONSANTO, as data controller, should have governed the processing carried

out on its behalf by its data processor by a legal act, especially by providing guarantees regarding data security.

On 29 October, the French SA issued a fine of EUR 400,000 on the controller RATP. The SA concluded the existence of a violation of Art. 5(1)(c) and (2) GDPR for the unnecessary data collection on strike days exercised by bus centre agents who were up for promotion. RATP had also breached Art. 5(1)(e) GDPR by failing to limit the duration of storing certain data of staff members, but it has managed to take necessary measures during the proceedings of the case to address this issue. The SA also found that the controller violated Art. 32 GDPR by not implementing appropriate security measures for data processing that can prevent any misuse of the data and guarantee confidentiality.

6.2.1.10. Germany

Germany has both a national (federal) SA and regional SAs. In 2021, an important case was dealt with by the Hamburg SA in which a fine of EUR 901,388.84 was imposed on the controller Vattenfall Europe Sales GmbH. The SA concluded that the controller breached its transparency obligations under Arts. 12 and 13 GDPR since it did not sufficiently inform the customers about the data comparison. Overall, this affected approximately 500,000 people. The SA further noted that the fine does not affect the question regarding the permissibility of comparison, which is not clearly regulated in the GDPR or any other legislation.

6.2.1.11. Greece

In a national case before the Hellenic SA, a sports trading company was fined EUR 20,000 for not erasing a complainant's phone number, although being requested to do so. This constituted a violation of Art. 17 GDPR in conjunction with Art. 21(3), Art. 12(3) and Art. 25(1) GDPR since the controller infringed on the data subject's right to erasure and did not ensure a correct procedure of ex-post fulfilment of that right.

The Hellenic SA issued a fine of EUR 15,000 to a company for illegally installing and operating a video surveillance system in the employees' offices and the kitchen of the workplace in breach of Art. 5(1)(a) and (2) GDPR. The company was also ordered to uninstall the cameras and delete any collected material.

An educational centre was issued two fines by the Hellenic SA for data protection violations. First, it imposed a fine of EUR 3,000 for a failure to satisfy the father's right of access to data of his minor child. Later on, the educational centre was fined an additional EUR 5,000 for non-compliance with the order of the Authority to satisfy the complainant's right of access.

In another case, the Hellenic SA issued two fines to the controller Municipal Transportation Company for breaching data protection rules. It fined the controller EUR 5,000 for breaching Art. 12(3) and Art. 15 GDPR by not fulfilling the complainant's right of access to a copy of recorded video material. The second fine amounted to EUR 3,000 as a result of infringement on the principle of proportionality, guaranteed under Art. 5(1)(c) GDPR, when the controller provided the complainant with the service certificate he requested after his dismissal from the company, but added therein that the complainant was fired as a result of a criminal offence.

6.2.1.12. Hungary

This section sets out seven pertinent instances in which the Hungarian SA imposed numerous fines for violations of data protection law.

On 29 September 2020, the Hungarian SA handled a case concerning sound recordings of customers at a controller's Customer Service Office. The controller argued that it informed its customers about the sound recordings through the number allocation system, in the general information accessible on its website and the Privacy Statement constituting an annex to its General Terms and Conditions of Contract. The SA concluded that the company did not have an appropriate legal basis for recording its customers and failed to take into consideration the customers' right to object. It further noted that in light of the absence of identification and clarity, the sound recording by the controller failed to comply with the principle of purpose limitation. The SA also found a breach of the principle of data minimisation since recordings were conducted throughout the entire process of administering personal cases and a breach of the principle of transparency due to the provided information by the controller which was deficient and comprised of misleading statements.

On 9 December 2020, a controller of the financial service sector was fined EUR 5,448 by the Hungarian SA. The decision was based on an infringement of Art. 32(1) GDPR since the controller did not implement sufficient data security measures for the processing of personal financial data.

In another case on the same day, the Hungarian SA established violations of Art. 25, Art. 32 and Art. 34 GDPR by a travel agency since it had entrusted the design of the website to an inadequate data processor, could not guarantee the security of the personal data processed and did not inform the data subjects about a high-risk data breach. In addition, the processor also violated Art. 32 GDPR since it failed to implement appropriate security checks on the website and acted with a high degree of negligence towards the website's development. Consequently, the controller was fined EUR 55,000 and the processor was fined EUR 1,375.

On 16 December 2020, the Hungarian SA issued a fine of EUR 98,600 on the controller, a bank, for breaching Art. 5(1)(c), Art. 6, Art. 9 and Art. 12(1) GDPR. The SA found that the bank, when processing copies of pregnancy care books, has processed some personal and special category personal data that was neither suitable, nor necessary for the purpose of the processing. The bank also did not have any legal basis for processing part of the data and it failed to provide unambiguous and transparent information on the processing of the personal data included in the copies of the pregnancy care books. Apart from the issued fine, the SA order the bank to annihilate the copies of the pregnancy care books and to transform the information provided on its processing.

On 24 March 2021, the Hungarian SA concluded the existence of several data protection violations by the Budapest Capitol's Government Office's XI. District Office. The infringement of Art. 32(1)(a), (b) and (2) GDPR was based on the insufficient application of data security measures by the controller regarding the transfer of medical data, which resulted in the possibility of causing a high-risk data breach. The controller violated Art. 33(1) GDPR when it did not consider it necessary to report the high-risk personal data breach to the Hungarian SA since it did not carry out the risk analysis properly. The violation of Art. 34(1) GDPR occurred since the controller did not communicate the high-risk data breach to the data subjects. A fine of HUF 10,000,000 (approximately EUR 28,000) was imposed on the controller.

On 18 June 2021, the Hungarian SA imposed a fine of EUR 13,705 and ordered the erasure of the data processed to an electronic media content service provider for multiple GDPR infringements. In this case, the controller published

personal and health data of a minor, making him identifiable, although that was not necessary for achieving the purpose of broadcasting news. Furthermore, the controller published the data without any legal basis since it did not acquire consent and it disregarded the preliminary objection of providing consent by the data subject's relative. The SA also found that the controller acted contrary to the principle of fair data processing by broadcasting news about a data subject who was physically incapacitated and therefore unable to express intent to consent or object to such processing.

On 27 October 2021, the Hungarian SA handled a case in which the data subject was not informed by the controller or processor of the data processing. In addition, the SA concluded that the processor did not have any legal basis for processing data that fell outside the scope of essential data for complaint management purposes. Consequently, the SA determined the existence of numerous violations of the GDPR, imposed a fine and requested a modification of the data processing.

6.2.1.13. Iceland

The Icelandic SA dealt with a number of cases, with some of them focusing on COVID-19.

On 15 June, the Icelandic SA issued a fine of EUR 34,000 on the controller Huppuís ehf., a company running ice cream parlours. The SA found that the processing of the employee's personal data via video surveillance camera installed in an employee area was not lawful, fair or transparent, nor adequate, relevant and limited to what was necessary in relation to the purposes for which the data was processed.

On 23 November, the Icelandic SA concluded that the conducted data protection impact assessment (DPIA) concerning the move of the microbiology department of the controller, the National University Hospital of Iceland, to the sub-processor, the company Decode Genetics, did not fulfil the GDPR requirements. Nevertheless, the SA established that nothing indicated non-compliance with the GDPR in relation to the security of personal data processed on the premises of Decode Genetics.

On the same day, 23 November, the Icelandic SA also decided on another case involving the same actors, the National University Hospital of Iceland and the company Decode Genetics. In this case, the SA determined that the processing of personal data by the two actors was not in compliance with the GDPR due to a lack of approval from the National Bioethics Committee. However, bearing in mind the urgency and importance of the work surrounding COVID-19, the SA decided not to issue fines in this case.

The Icelandic SA handled a third case revolving around the same actors on 23 November. In this case, the controller was the National Chief Epidemiologist who was ordered to update the processing agreement with the National University Hospital of Iceland so that the agreement would be in line with Art. 28 GDPR. Comparable to the previous case, in this case the SA also did not issue fines in light of the urgency and importance of the work surrounding COVID-19.

One day after, on 24 November, the Icelandic SA imposed a fine of ISK 7,500,000 (approximately EUR 50,800) on the controller, the Ministry of Industries and Innovation of Iceland, and imposed a fine of ISK 4,000,000 (approximately EUR 27,100) on the processor, the company YAY ehf. The case revolved around a digital gift card app that unlawfully and unnecessarily collected substantial amounts of personal data and acquired access rights to the user's mobile devices.

The SA determined that consent was given by the app users and there was a lack of information transparency. In addition, the controller and the processor had not ensured the appropriate security of the personal data, had not made a processing agreement and had not implemented data

protection by design and by default that could have ensured data minimisation.

6.2.1.14. Ireland

The Irish SA, on its own volition, started an inquiry into the Department of Employment Affairs and Social Protection after receiving a complaint from Digital Rights Ireland. The SA concluded no infringement of Art. 38(1) GDPR since the Department involved their DPO properly and in a timely manner in the Department's amendment of its Privacy Statement. No violation of Art. 38(3) GDPR was either found because the Department did not provide any instructions to the DPO regarding the exercise of their tasks contrary to the GDPR.

The Irish SA imposed a fine of EUR 90,000 on the controller, the Irish Credit Bureau DAC (ICB). The ICB violated Art. 25(1) GDPR by failing to implement appropriate technical and organisational measures designed to implement the principle of accuracy effectively and to integrate the necessary safeguards into the processing. A violation of Art. 5(2) and Art. 24(1) GDPR was also established for the ICB's failure to demonstrate compliance with its obligation to undertake appropriate testing of proposed changes to its database. The ICB was issued a reprimand as a result of the committed violations.

In another case, The Irish SA reprimanded and imposed a fine of EUR 1,500 to the controller, Men Overcoming Violence (MOVE) for infringing upon Art. 5(1)(f) and Art. 32(1) GDPR. The SA decided that MOVE failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing by means of recording group sessions on SD Cards containing participants' and facilitators' personal data. The controller was ordered to bring its processing into GDPR compliance.

6.2.1.15. Italy

In January, the Italian SA concluded various violations by TikTok in relation to poor attention to the protection of minors on account of the easy circumvention of its age gating mechanism, the distribution of unclear information to users and the poor adherence to privacy requirements by the application's default settings. TikTok was ordered to implement appropriate access limitation measures for minors (below the age of 14) and was prohibited from further processing personal data of users whose age can't be verified.

In February, a case concerning data of applications for a COVID-related bonus was handled by the Italian SA in which a EUR 300,000 fine was issued to the National social security agency (INPS). The SA concluded that the processing by INPS was unlawful. INPS was ordered to erase unnecessary data and carry out an appropriate DPIA.

In April, the Italian SA did not issue a favourable opinion on the use of facial recognition technology through the SARI Real Time system to support law enforcement activities of the controller, the Italian Ministry of the Interior. The SA concluded a lack of legal basis to legitimise the automated processing of biometric data for facial recognition in security applications, particularly because it will enable a mass/blanket surveillance.

In June, the Italian SA issued several corrective measures and a fine of EUR 2,600,000 on the controller Foodinho s.r.l. for several infringements of the GPDR and national law provisions. The corrective measures focused on issues such as transparency, data processing, DPIA, data storage, fairness and accuracy of an algorithm that avoids discrimination, data minimisation, employment and work surveillance.

In the same month, the Italian SA determined that the configuration of the 'IO' application of the controller PagoPA Spa, infringed on the GDPR. The controller made commitments to minimise the excessive data collection and transfer to third countries and to implement corrective measures that would remedy the infringements found. As a consequence, the Italian SA decided to lift the previously imposed temporary limitation on the processing of personal data via the 'IO' app.

In July, the Italian SA imposed a fine of EUR 2,500,000 on the controller Deliveroo Italy s.r.l. for the poor transparency in using algorithms and the disproportionate collection of employees' data. The SA also issued numerous corrective measures concerning issues such as transparency, processing records, DPIA, data storage, data safeguards, fundamental freedoms and legitimate interests, fairness and accuracy of an algorithm that avoids discrimination, data minimisation, employment and work surveillance.

Later in September, the Italian SA reprimanded a real estate agency for exchanging information with a data subject on LinkedIn that was contrary to the platform's Terms of Service. The SA determined that the processing was unlawful and ordered the real estate agency to take suitable organisational measures. Nonetheless, the SA imposed a fine of EUR 5,000 on the controller for its failure to reply to the SA's repeated requests for information.

In the same month, the Italian SA ordered Sky Italia to pay a fine of over EUR 3,200,000 and banned any further processing for promotional purposes of telephone subscribers' data the company had obtained from other entities. Sky Italia was also ordered to make a certified email account that will facilitate opt-out requests by data subjects and to appoint all the entities that perform promotional activities on its behalf as data processors whilst Sky, as a controller, supervises the activities of the processors and verify the proper management of users' information. Interestingly, the Italian SA noted that the calculation of the fine took into account the gravity of the violations that were grounded in "systematic" practices at a corporate level.

6.2.1.16. Latvia

On 14 January, the Latvian SA impose a fine of EUR 65,000 on a data re-user for ensuring public access to data even after the applicable regulatory enactments required to restrict access to such data.

On 14 May, the Latvian SA issued a fine of EUR 100,000 against an online retailer that carried out processing of personal data to identify a natural person without legal basis. The controller was ordered to delete the personal data – copies of imagines of user's documents – from its website. The decision has been appealed and is still pending.

6.2.1.17. Liechtenstein

A private insurance company was found in violation of Art. 6(1)(a), Art. 7 and Art. 13 GDPR for unlawfully obtaining and processing personal data of data subjects. The company was banned from processing the data and was ordered to erase the collected data.

A Swiss company, acting as a controller, was ordered to erase personal data consisting of unlawfully recorded phone calls in Liechtenstein. Even though the controller is established in Switzerland, the SA concluded an infringement of Art. 6(1) GDPR since no consent was obtained from the EEA nationals.

6.2.1.18. Lithuania

The Lithuanian SA handled a number of cases in 2021. A selection of those cases is presented in this section.

Upon a conducted investigation, the Lithuanian SA imposed a fine of EUR 12,000 to the National Public Health Centre (NPHC) and a fine of EUR 3,000 to the developer of the application UAB "IT sprendimai sėkmei" (the Company). The two entities acted as joint controllers who processed personal data intentionally, to a large extent, illegally, systematically, without providing technical and organisational means to demonstrate GDPR compliancy while conducting such processing, and they also processed special category personal data.

The Lithuanian SA issued a fine of EUR 15,000 to the State Enterprise Centre of Registers for infringements of Art. 32(1) (b) and (c) GDPR. The controller in this case failed to ensure the ongoing integrity, availability and resilience of processing systems and services, but also failed to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

A case before the Lithuanian SA concerned the processing of biometric personal data in a sports club that resulted in a EUR 20,000 fine for the controller, VS FITNESS UAB. The controller was deemed in violation of numerous GDPR provisions for processing biometric data without the voluntary consent of the data subjects and its failure to ensure other requirements for the valid consent, the unsuitable implementation of the data subjects' right to be informed of data processing, the failure to maintain records of activities and not conducting a DPIA.

One of the cross-border cases before the Lithuanian SA involved the company Prime Leasing UAB, an operator of the short-term car rental platform CityBee, that was fined EUR 110,000 for breach of Art. 32(1)(a), (b) and (d) GDPR. The violation was mainly grounded on the fact that the company did not ensure the security of the processing of personal data of data subjects.

6.2.1.19. The Netherlands

In 2020 and 2021, the Dutch SA imposed multiple fines for GDPR violations. Most of the fines were imposed because of serious breaches of data subjects' rights. Selected cases are listed here:

- In March 2020, the maintenance company CP&A B.V. was fined EUR 15,000 for violations committed when processing the health data of sick employees. The company maintained a register of the causes of sick leave, which resulted in processing more health data than legally permitted. Moreover, this register was accessible online and not adequately secured. CP&A has now ended this practice;
- In June 2020, the Dutch SA fined PVV Overijssel an amount of EUR 7,500 for failing to report a data breach to the SA within the applicable time limit – within 72 hours of becoming aware of the data breach;
- In November 2020, the Dutch SA determined a fine of EUR 440,000 for the Amsterdam-based hospital OLVG for its inadequate protection of patients' medical records. The SA established that OLVG did not implement sufficient safeguards to prevent unauthorised access to the records, it did not carry out proper checks of who accessed which records and did not address problems pertaining to the information systems security. Consequently, OLVG worked on the required improvements;
- In March 2021, the Dutch SA issued a fine of EUR 600,000 to the municipality of Enschede for using Wi-Fi tracking in the city centre in a way that is prohibited. Following the intervention by the SA, the municipality stopped such data tracking on 1 May 2020;
- In April 2021, the Dutch SA imposed a fine of EUR 750,000 on TikTok for infringing on young children's privacy. TikTok lodged an objection to the fine. During the course of the investigation, TikTok established operations in Ireland.

As a result, the Dutch SA transferred other results of the investigation to the Irish SA, which will proceed with the investigation on TikTok's processing operations;

- A month later, in May, the Dutch SA imposed a EUR 450,000 fine on the Employee Insurance Agency (UWV) for the poor security when sending group messages via the "Mijn Werkmap" section of its website, a personal environment in which job seekers can interact with the UWV. The website has suffered multiple data breaches that involved personal and health data of more than 15,000 data subjects;
- In June 2021, the Dutch SA issued a fine of EUR 12,000 to an orthodontic practice for allowing new patients to register on an unsecured website. This could have led to an unwanted third-party breach of patients' sensitive personal data, such as their citizen service number;
- In December 2021, the Dutch SA imposed a EUR 2,750,000 fine on the Dutch Tax Administration because for many years it processed data on the dual nationality of childcare benefit applicants in an unlawful, discriminatory and improper manner.

6.2.1.20. Norway

The Norwegian SA issued multiple fines in 2021. The Norwegian SA carried out the following actions:

- Imposed a fine of EUR 15,000 on the controller Dragefossen AS for live streaming CCTV surveillance recordings of data subjects that were in no way, personally or their activities, connected to the controller;
- Issued a fine of approximately EUR 500,000 to the Norwegian toll company Ferde AS for failing to establish a data processing agreement, to carry out a risk assessment and its lack of legal basis for the processing of personal data about motorists in China;
- Imposed a fine of EUR 100,000 to the controller Innovation Norway for lacking a legal basis of processing personal and financial data in relation to credit rating;
- Imposed a fine of EUR 125,000 to the controller Norwegian Confederation of Sport for inadequate testing involving personal data. The controller did not have a legal basis for processing the data and overall breached the principles of legality, data minimisation and confidentiality;
- Ordered the company Cyberbook AS to implement written procedures for access to the email inboxes of employees and former employees, but also imposed a EUR 20,000 fine for the unlawful automated forwarding of the employee's personal email address to the company;
- Ordered the Oslo University Hospital to amend data processing agreements and therefore ensure the correct handling of the hospital's duties and the protection of patients' rights;
- Issued a fine of approximately EUR 6,500,000 to Grindr LLC for disclosing user data to third parties for behavioural advertisement without a legal basis. The SA concluded that the purported consents that were collected for sharing personal data with advertising partners were not valid. Furthermore, Grindr failed to properly communicate the sharing of personal data to its users. Notably, the SA considered that the sensitive nature of the shared data – belonging to a sexual minority – makes the data a special category data that merits particular protection under the GDPR.

6.2.1.21. Poland

The Polish SA handled several cases in 2021. One violation that was consistently addressed by the SA was the controllers' failure to notify personal data breaches to the SA. This can be observed in some of the cases presented in this section.

On 11 January, the Polish SA imposed a EUR 30,000 fine on the controller ENEA S.A. for failing to notify a personal data breach once personal data has been accidentally shared with an unauthorised recipient of such data. The breach consisted of a shared email that had an unencrypted, non-password protected attachment containing personal data of several hundred people.

On 11 February, the Polish SA issued a fine of EUR 22,000 to the National School of Judiciary and Public Prosecution (KSSIP) for failing to fulfil its obligations as a controller. While the processor was found to be in compliance with the GDPR rules, the controller breached the confidentiality of data subjects by failing to conduct an analysis of whether it was exposing personal data stored in a database that was shared with the processor.

On 19 March, the Polish SA issued a fine of EUR 5,000 to the company Funeda Sp. z o.o. for its failure to cooperate with the SA, in particular the impediment of access to necessary information.

On 22 April, the controller Cyfrowy Polsat S.A. was fined EUR 250,000 for the lack of implementation of adequate organizational and technical measures for detecting data breaches that should result in the prompt notification to data subject of the risk associated with potential identity theft.

A few days later, on 27 April, the company PNP S.A. was fined EUR 5,000 for violating its obligation of providing access to information to the Polish SA, especially information that was necessary to address the merits of the case.

On 8 June, the Polish SA imposed a fine of EUR 22,000 on the controller P4 Sp. z o.o. for its failure to notify the SA of personal data breaches. The controller did not manage to meet the notification deadline due to employees' errors when dispatching data breach notifications to data subjects through postal service – a method of notification that was persistently held on to by the controller, although having the opportunity to dispatch electronic notifications.

On 21 June, the Polish SA imposed a fine of EUR 35 000 on the company ERGO Hestia S.A. for failing to notify the SA of a security breach when personal data was made available to an unauthorised recipient that was considered to be untrusted.

On 14 October, the bank Millennium was fined EUR 80,000 for its failure to notify a personal data breach to the SA and also for not communicating it to the data subjects. Consequently, in line with Art. 34(2) GDPR, the bank was ordered to communicate the data breach to the persons affected by it.

6.2.1.22. Romania

In October, the Romanian SA issued a reprimand and remediation measures against Cluj-Napoca City for violation of Art. 15(3) and Art. 12(3) and (4) GDPR. The remediation measures consisted of implementing an internal procedure for processing requests submitted by data subjects based on the GDPR, the observance of the applicable provisions regarding the assessment and handling without delay of these requests and communication of answers to the data subjects within the legal deadlines, but also conducting regular personnel training in relation to this.

In April, the controller World Class România S.A. was sanctioned with a EUR 2,000 fine for the violation of Art. 32 GDPR concerning the insufficient security of the processing of personal data. Additionally, the SA issued a corrective measure that ordered the controller to ensure GDPR compliance of the processing (within 30 days of communicating the SA's decision) by implementing appropriate technical and organisational measures in case of remote transmission of the personal data, but also to conduct regular personnel training in respect to this.

In the same month, the controller Telekom Romania Communications S.A. was reprimanded for violation of Art. 6 GDPR since it processed personal data for marketing purposes without a legal basis. The controller was also fined EUR 2,000 for violation of Art. 21 GDPR since it had contacted by phone a data subject, who had previously exercised their right to object.

Later in October, the Romanian SA imposed a fine of EUR 1,000 on the controller IKEA ROMÂNIA SA for infringing on Art. 32(1)(b) and (2) GDPR when a data breach occurred that resulted in compromising the data confidentiality of 114 Ikea Family members.

In November, the Romanian SA took several corrective measures against UAT Municipiul Constanța for possible breach of the data minimisation principle, guaranteed under Art. 5(1)(c) GDPR. The measures consisted of a reprimand for violating Art. 5(1)(c) GDPR and an order to take necessary measures to observe the data minimisation principle in relation to issuance of car access permits for its residents, including through the amendment of the Local Council Decision regarding this processing.

6.2.1.23. Slovenia

The Slovenian SA handled several cases in 2020 and 2021. A few cases of particular importance are presented in this section.

The controller National Institute of Public Health was ordered to provide clear, accurate and reliable information on registration for vaccination per Art. 13 GDPR. As a result, the controller informed the data subjects about its function as a data controller, the purpose of data processing, the legal basis, the storage period and the data subject rights.

The Slovenian SA determined that a controller unlawfully monitored work areas through video surveillance. As a result, the controller was ordered to remove the surveillance cameras, with a few exceptions (e.g., the warehouse). The SA also found that the controller failed to ensure traceability of the data processing since it did not keep data records.

The Slovenian SA dismissed a complaint of a data subject that requested the erasure of his personal information from the Baptismal Register of a parish of the Roman Catholic Church. The SA concluded that the right to erasure, guaranteed under Art. 17 GDPR, does not enable an individual to have their personal data erased from the register. The complainant challenged the decision before the national justice system, but nonetheless, the Slovenian Administrative Court upheld the decision of the SA.

The Slovenian SA decided to dismiss a complaint of a patient to rectify a medical report. The SA elaborated that this right enables data subjects to rectify data that is not accurate, while that was not the situation in the case at hand. Concerning the principle of accuracy, the SA stated that the controller is processing accurate personal data of the individual, particularly considering the amendment of the initial medical report that contains additional text, while not deleting previously written text.

A decision of the Slovenian SA determined that a restaurant is not allowed to monitor the movements of individuals across the restaurant through video surveillance. The SA stressed that the safety in the restaurant can be achieved by less privacy intrusive measures, such as monitoring only specific areas like the cash register and the entry. In addition, the SA emphasised that the video surveillance should not be managed by the work supervisors, but rather by security officers.

A series of cases concerning positive infections of the COVID-19 virus resulted in infringements of various GDPR rules. The Slovenian SA found that one state authority violated Art. 5(1) (c) GDPR when informing other employees about co-workers who tested positive to the COVID-19 virus. Moreover, in all three cases, the controller did not inform the employees, who were COVID-19 positive, about the processing of their data, which resulted in the violation of Art. 13 GDPR. In one of the cases, the state authority was issued a fine of EUR 830 and an administration fee in the amount of EUR 83 for processing personal data of an employee without their consent or determination for such processing.

6.2.1.24. Spain

The Spanish SA issued a number of comparable fines in late 2020 and throughout 2021. The Spanish SA carried out these actions:

- Imposed a fine of EUR 500,00 on the controller EDP ENERGIA, S.A.U. for violating Art. 25 GDPR by not adopting appropriate technical and organisational measures for processing personal data. The controller was also fined EUR 1,000,000 for violating Art. 13 GDPR since it did not adequately provide information to data subjects;
- Issued multiple fines that together amount to more than EUR 8,000,000 (highest fine amount issued by the SA) to the controller Vodafone España, S.A.U. In particular, it imposed a fine of EUR 4,000,000 for infringement of Art. 28 GDPR, a fine of EUR 2,000,000 for infringement of Art. 44 GDPR and two fines in the amount of EUR 2,000,000 and EUR 150,000 for violation of two national laws – General Telecommunications Law and Electronic Commerce Law. Apart from this, the SA also order the controller to bring its processing operations into compliance with Art. 17, Art. 21, Art. 24, Art. 28 and Art. 44 to Art. 49 GDPR within six months of the adoption of the decision;
- Imposed a fine of EUR 2,520,000 on MERCADONA, S.A. for the use of a non-legitimised facial recognition system in supermarkets, as well as for lack of transparency, excessive use of personal data, lack of privacy by design and poor impact assessment;
- Issued to the controller EDP ENERGÍA, S.A.U. a fine of EUR 500,000 for violation of Art. 25 GDPR and a fine of EUR 1,000,000 for violation of Art. 13 GDPR;
- Decided to close a case due to the non-infringement of the GDPR. The SA determined that medical data of patients belong to the hospital, the controller, and not to the doctor who treated the patients while working at the hospital;
- Issued a fine of EUR 1,500 to a natural person for posting photographs and notes of sexual content of their partner on a website without the consent of the partner;
- Imposed a total fine of EUR 6,000,000 on CAIXABANK, S.A., for unlawfully processing clients' personal data (in the amount of EUR 4,000,000) and not providing sufficient information regarding the processing of personal data (EUR 2,000,000). Apart from the issued fine, the Spanish SA ordered CAIXABANK to bring its processing operations into compliance with Art. 6, Art. 13 and Art. 14 GDPR within six months of the adoption of the decision;
- Issued a fine of EUR 3,000,000 to the controller CAIXABANK PAYMENTS & CONSUMER EFC, EP, S.A.U. for lack of specific and informed consent regarding profiling for commercial purposes. In addition, the controller was ordered to bring its processing operations in compliance with the GDPR within six months of the adoption of the decision.

6.2.1.25. Sweden

In 2021, the Swedish SA conducted numerous enforcement measures for violations of the GDPR, some of which

concerned Swedish national authorities. This is illustrated in the cases outlined here.

On 10 February, the Swedish Police Authority was fined EUR 250,000 for breaching the Criminal Data Act (which implements the EU Law Enforcement Directive 2016/680) by using the biometric data tracking application Clearview AI in its operational activities. The Police were ordered to ensure the erasure of data that was transferred to Clearview AI, to inform affected data subjects that their data had been processed by Clearview AI and to conduct personnel training and education in respect to avoiding similar future processing of personal data that is unlawful. The Police decided to appear the decision, which is now to be settled by the Swedish Administrative Court of Appeal.

On 7 June, the Swedish SA issued multiple fines in a case concerning the unprotected web availability of recorded phone calls in relation to medical consultations. The SA imposed a fine of EUR 1,200,000 on the controller Medhelp for its failure to take appropriate security measures, for the lack of provided information to data subjects and for breaching certain provisions of the Swedish health and medical care legislation. The SA imposed a EUR 50,000 fine on Voice Integrate for failing to take appropriate and sufficient security measures to protect phone calls handled on behalf of Medhelp. In addition, the SA issued EUR 50,000 fine on three regional authorities for not providing sufficient information to the data subjects seeking medical care through the service. The decisions of the SA have been appealed and are to be settled by the Swedish Administrative Court of Appeal.

On 9 June, the Swedish SA issued a fine of EUR 34,000 against the Executive Board of the Rescue Service in Östra Skaraborg (Rescue Service). While the SA established that the Rescue Service has compelling reasons for its camera surveillance, it should limit the recording to events when the alarm is activated and should mask areas where firefighters change clothes in order to capture only necessary information. The Rescue Service has stopped the camera surveillance.

On 21 June, the Swedish SA imposed a EUR 15,500,000 fine to the public transport operator Storstockholms Lokaltrafik (SL) for the infringements of Art. 5, Art. 6 and Art. 13 GDPR. The SA concluded that the authority needs to reduce the pre-recording time on the body-worn cameras for threat prevention to 15 seconds. It also found that the technology should not be used for the identification of passengers without tickets and added that still images and soundless recordings are sufficient for the purpose of threat prevention. The controller also failed to adequately inform about the camera surveillance, in particular that, apart from video, sound was also recorded.

6.3. SA BUDGET AND STAFF

The EDPB received a request from the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) of the European Parliament to share some statistics on resources made available by Member States to the SA from the EEA and on enforcement actions by the SAs. The EDPB already gathered similar information in the past in the context of a 2019 Report about the GDPR implementation made at the request of the LIBE Committee and the contribution of the GDPR evaluation made in 2020 at the request of the European Commission.

On 5 August 2021, the EDPB published an "Overview of the resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities". The vast majority of SAs (22) explicitly stated that their allocated budget is not sufficient for carrying out the work activities. Based on the information from 29 SAs from EEA countries before August 2021, six SAs even faced a budgetary decrease in comparison to their 2020 budget.

In respect to SAs' human resources, a vast majority of SAs (22) underlined the fact that they do not have enough human resources to face their workload. Ten SAs did not experience any change in their staff numbers, while six SAs saw a decrease in employees in 2021, in comparison to 2020.

The document providing the overview of the SAs' resources also demonstrates that, across the majority of the SAs, a greater number of staff usually works on national enforcement cases in comparison to cross-border cases.

In its contribution to the evaluation of the GDPR adopted in 2020, the EDPB stressed that the effective application of the powers and tasks attributed by the GDPR to SAs is largely dependent on the resources available to them.

7

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

In accordance with Art. 62 of Regulation 2018/1725, the national Supervisory Authorities (SAs) and the European Data Protection Supervisor (EDPS) shall cooperate actively to ensure effective supervision of large-scale IT systems and of EU bodies, offices and agencies. For this purpose, they shall meet at least twice per year within the framework of the EDPB. Additionally, several legal acts on large-scale IT systems and EU agencies refer to this model of coordinated supervision.

To ensure the consistency of supervision efforts on both levels, all SAs involved, including the EDPS, used to cooperate through Supervision Coordination Groups (SCGs).[4] Each of these groups was dedicated to a specific EU database. Since December 2018, Regulation 2018/1725 has provided for a single model of coordinated supervision for large-scale EU IT systems and agencies within the framework of the EDPB. This replaces the current system of individual SCGs. The new model does not apply to all EU information systems and agencies at once, but progressively, according to when the revised version of the establishing act of each EU information system and agency becomes applicable.

In December 2019, the Coordinated Supervision Committee (CSC) was formally established within the EDPB. It brings together the SAs of each EU Member State and the EDPS, as well as SAs of non-EU Members of the Schengen Area where provided for in EU law.

The CSC's tasks include, among others, supporting SAs in carrying out audits and inspections; working on the interpretation or application of the relevant EU legal act; studying problems within the exercise of independent supervision or within the exercise of data subject rights; drawing up harmonised proposals for solutions; and promoting awareness of data protection rights.

Participation in the CSC meetings can occur under various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act. As announced in December 2020, during its third plenary meeting, the CSC elected Clara Guerra from the Portuguese SA to succeed Giuseppe Busia as its new Coordinator for a term of two years. Sebastian Hümmeler from the German Federal SA currently holds the position of Deputy Coordinator.

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

Internal Market:

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

Police and Judicial Cooperation:

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

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

Border, Asylum and Migration:

- Schengen Information System (SIS), ensuring border control cooperation (expected no later than June 2022);
- Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen States (expected before the end of 2022);
- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone (expected in May 2023);
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States (expected by the end of 2023);
- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State (expected in 2022);
- Customs Information System (CIS), which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation.

Police and Judicial Cooperation:

- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked (expected for 2022);
- Europol, the EU's law enforcement agency (expected in 2022);
- Schengen Information System (SIS) (see above, as this system also fall under Police and Judicial cooperation).

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

8

ANNEXES

8.1. GENERAL GUIDANCE ADOPTED IN 2021

- Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- Guidelines 08/2020 on the targeting of social media users
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679
- Guidelines 10/2020 on restrictions under Art. 23 GDPR
- Guidelines 01/2021 on examples regarding data breach notification
- Guidelines 02/2021 on virtual voice assistants
- Guidelines 03/2021 on the application of Art. 65(1)(a) GDPR
- Guidelines 04/2021 on codes of conduct as tools for transfers
- Guidelines 05/2021 on the interplay between the application of Art. 3 and the provisions on international transfers as per Chapter V of the GDPR
- Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Arts. 42 and 43 of the Regulation)
- Recommendations 01/2020 on measures that supplement

transfer tools to ensure compliance with the EU level of protection of personal data

- Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive
- Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions

8.2. CONSISTENCY OPINIONS AND DECISIONS ADOPTED IN 2021

- Opinion 01/2021 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Saxo Bank Group
- Opinion 02/2021 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Elanders Group
- Opinion 03/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of BDO
- Opinion 04/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of BDO
- Opinion 05/2021 on the draft Administrative Arrangement for the transfer of personal data between the Haut Conseil du Commissariat aux Comptes (H3C) and the Public Company Accounting Oversight Board (PCAOB)
- Opinion 06/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of Kumon Group
- Opinion 07/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Kumon Group
- Opinion 08/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Processor Binding Corporate Rules of Luxoft Group
- Opinion 09/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Controller Binding Corporate Rules of Luxoft Group
- Opinion 10/2021 on the draft decision of the competent Supervisory Authority of Hungary regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 11/2021 on the draft decision of the competent Supervisory Authority of Norway regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 12/2021 on the draft decision of the competent Supervisory Authority of Portugal regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 13/2021 on the draft decision of the competent Supervisory Authority of Romania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the “EU Data Protection Code of Conduct for Cloud Service Providers” submitted by Scope Europe
- Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE)
- Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the Lithuanian Supervisory Authority (Art. 28(8) GDPR)
- Opinion 19/2021 on the draft decision of the competent

Supervisory Authority of Hungary regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR

- Opinion 21/2021 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the CGI Group
- Opinion 22/2021 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the CGI Group
- Opinion 23/2021 on the draft decision of the competent Supervisory Authority of Czech Republic regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 24/2021 on the draft decision of the competent Supervisory Authority of Slovakia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 25/2021 on the draft decision of the competent Supervisory Authority of Lithuania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 26/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Controller Binding Corporate Rules of the Internet Initiative Japan Group
- Opinion 27/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Processor Binding Corporate Rules of the Internet Initiative Japan Group
- Opinion 28/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Oregon Tool, Inc (formerly "Blount")
- Opinion 29/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of Oregon Tool, Inc (Formerly "Blount")
- Opinion 30/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the COLT Group
- Opinion 31/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group
- Opinion 33/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Carrier
- Opinion 34/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Otis
- Opinion 35/2021 on the draft decision of the competent Supervisory Authority of Belgium regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 36/2021 on the draft decision of the competent Supervisory Authority of Norway regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 37/2021 on the draft decision of the competent Supervisory Authority of Malta regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 38/2021 on the draft decision of the competent Supervisory Authority of Latvia regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 39/2021 on whether Art. 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject

- Urgent Binding Decision 01/2021 on the request under Art. 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited
- Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Art. 65(1)(a) GDPR

8.3. JOINT OPINIONS ADOPTED IN 2021

- EDPB-EDPS Joint Opinion 01/2021 on standard contractual clauses between controllers and processors
- EDPB-EDPS Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries
- EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)
- EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery
- EDPB-EDPS Joint Opinion 05/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

8.4. LEGISLATIVE CONSULTATION

- Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom
- Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom
- Opinion 20/2021 on Tobacco Traceability System
- Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea
- EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research – 02/02/2021
- EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime – 04/05/2021
- Statement 05/2021 on the Data Governance Act in light of the legislative developments – 19/05/2021
- Statement on the Digital Services Package and Data Strategy – 18/11/2021
- Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62 – 14/12/2021

8.5. OTHER DOCUMENTS

- Information note on data transfers under the GDPR to the United Kingdom after the transition period - update 13/01/2021
- Statement on the end of the Brexit transition period - update 13/01/2021
- Pre-GDPR BCRs overview list – 26/01/2021
- EDPB Work Programme 2021/2022 – 16/03/2021

8.6. LIST OF EXPERT SUBGROUPS WITH SCOPE OF MANDATES

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
Borders, Travel & Law Enforcement (BTLE) Expert Subgroup	• 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 (CEH) Expert Subgroup	• 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	• 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 GDPR outside the EU (Art. 50 GDPR)
Coordinators Expert Subgroup	• General coordination between the Expert Subgroup Coordinators • Coordination on the annual Expert Subgroup working plan

Enforcement Expert Subgroup	• 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	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	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	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	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	• 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	• 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	Development of Guidelines on the harmonisation of the calculation of fines
Technology Expert Subgroup	• 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