2020 ANNUAL REPORT

ENSURING DATA PROTECTION RIGHTS IN A CHANGING WORLD

edpb

European Data Protection Board

ENSURING DATA PROTECTION RIGHTS IN A CHANGING WORLD

An Executive Summary of this report, which provides an overview of key EDPB activities in 2020, is also available.

Further details about the EDPB can be found on our website at edpb.europa.eu.

TABLE OF CONTENTS

9

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.
COVID-19 contact tracing	A process to identify individuals who have been in contact with those infected by disease, such as COVID-19.
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 or 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.

Foreword

2020 and the COVID-19 pandemic made for a particularly challenging year. The pandemic and resultant lockdowns significantly altered how we live and work. They also drew attention to the nature of our fundamental rights and interests, not least the rights to privacy and data protection. Given the increasing presence of data-driven technologies in addressing the pandemic and its related challenges, the awareness of data protection rights among individuals and organisations has never been more critical.

It is important to note that the 2020 lockdown did not mean a slowdown of the EDPB's activities. On the contrary, the EDPB Secretariat organised a substantially higher number of EDPB meetings in response to these circumstances. The EDPB held 172 plenary and expert subgroup meetings and 96 drafting team meetings between rapporteurs drafting EDPB documents. We met more frequently (through our secured video platforms) and tackled a very heavy workload on top of what was already in our work programme for 2019 and 2020.

The EDPB worked quickly to respond to questions of how to process personal data in the context of the COVID-19 pandemic. We issued guidance on, amongst others, location and contact-tracing apps; processing health data for scientific research; restrictions on data subject rights in a state of emergency; and data processing in the context of reopening borders.

Aside from the pandemic and the data protection issues it raised, there were several major developments in the EU data protection legal sphere. The Court of Justice of the European Union's ruling in Schrems II had a significant impact on data exporters and more globally on any entity involved in international transfers of personal data. The EDPB immediately issued an FAQ document, followed later by our Recommendations for Supplementary Measures when using international transfer tools to ensure compliance with the EU level of personal data protection, which were subject to a public consultation. We received over 200 contributions from various stakeholders, showing the keen interest in the ruling and our related guidance.

In February 2020, the EDPB and national Supervisory Authorities (SAs) contributed to the European Commission's evaluation and review of the GDPR, as required by Art. 97 GDPR. Despite challenges, the EDPB is convinced that ongoing cooperation between SAs will facilitate a shared approach to data protection and establish consistent practices. We also believe it is premature to revise the GDPR at this point in time.

Our role includes contributing to the consistent interpretation of the GDPR by adopting Guidelines and Opinions. In 2020, we adopted 10 Guidelines on topics such as the concepts of controller and processor; and targeting of social media users, as well as three Guidelines in their final, post-consultation versions.

Next to providing guidance, ensuring consistency in enforcement and cooperation between national authorities is a key task of the EDPB. In 2020, we issued 32 Opinions under the Art. 64 GDPR consistency mechanism in areas with cross-border implications. Importantly, we successfully concluded the first dispute resolution procedure on the basis of Art. 65 GDPR. The EDPB also published its 'One-Stop-Shop' decision register online, which gives companies real case examples to guide their respective privacy project implementations.

We have recently adopted a new bi-annual work programme, which builds on the EDPB 2021-2023 Strategy. Some of the guidance we included in this work programme for the next two years is aimed at further streamlining cross-border enforcement of data protection law.

All our work was made possible thanks to the ceaseless efforts of everyone within the EDPB, in spite of the challenges that came with the COVID-19 pandemic. We also welcomed the increased input and engagement from our stakeholders through the seven public consultations we carried out in 2020, virtual events, workshops and surveys.

Since May 2018, and even well before that, we have constantly been trying to improve the implementation of the GDPR to ensure that the law achieves it intended results, namely an equally high level of data protection everywhere in the EEA. As we look forward to 2021, we will strive to contribute to a common data protection culture that ensures individuals enjoy the robust protection of their data protection rights.

Andrea Jelinek

Chair of the European Data Protection Board

2

About the European Data Protection Board: mission, tasks and principles

The European Data Protection Board (EDPB) is an independent European body, established by the General Data Protection Regulation (GDPR), which aims to ensure the consistent application of data protection rules across the European Economic Area (EEA).

It achieves this aim by promoting cooperation between national Supervisory Authorities (SAs) and issuing general, EEA-wide guidance regarding the interpretation and application of data protection rules.

The EDPB comprises the Heads of the EU SAs and the European Data Protection Supervisor (EDPS). The European Commission and - with regard to GDPR-related matters - the European Free Trade Association Surveillance Authority - have the right to participate in the activities and meetings of the EDPB without voting rights.

The SAs of the EEA countries (Iceland, Liechtenstein and Norway) are also members of the EDPB, although they do not hold the right to vote. The EDPB is based in Brussels.

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

2.1. MISSION

The EDPB has adopted a Mission Statement, whereby it aims to do the following:

- Ensure the consistent application of the GDPR and the Police and Criminal Justice Data Protection Directive across the EEA;
- Provide general opinions and guidance on European data protection laws to ensure the consistent interpretation of individuals' rights and obligations;
- Make binding decisions addressed to national SAs that ensure the consistent application of the GDPR;
- Act in accordance with its Rules of Procedure and guiding principles.

2.2. TASKS AND DUTIES

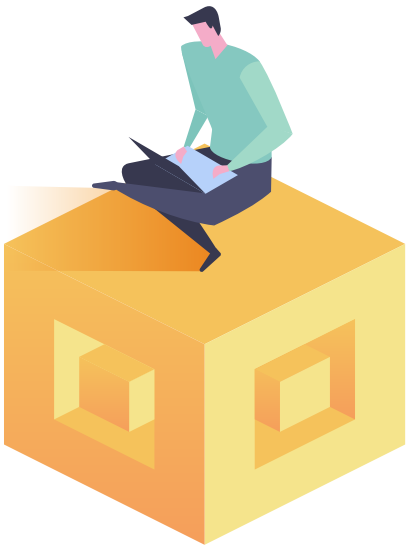
The EDPB has the following tasks and duties:

- Provide general guidance (including Guidelines, Recommendations and Best Practices) to clarify the law;
- Adopt Consistency Findings in cross-border data protection cases;
- Promote cooperation and the effective exchange of information and Best Practices between national SAs;
- Advise the European Commission on any issue related to the protection of personal data and proposed legislation in the EEA.

2.3. GUIDING PRINCIPLES

The EDPB actions are based on the following guiding principles:

- **Independence and impartiality.** The EDPB is an inde¬pendent body, which performs its tasks and exercises its powers impartially;
- **Good governance, integrity and good administrative behaviour.** The EDPB acts in the public interest as an expert, trustworthy and authoritative body in the field of data protection, with quality decision-making process¬es and sound financial management;
- **Collegiality and inclusiveness.** The EDPB acts collectively as a collegiate body pursuant to the GDPR and the Police and Criminal Justice Data Protection Directive;
- **Cooperation.** The EDPB promotes cooperation be¬tween SAs and endeavours to operate by consensus;
- **Transparency.** The EDPB operates as openly as possible to ensure efficacy and accountability to the public. The EDPB explains its activities in plain language that is accessible to all;
- **Efficiency and modernisation.** The EDPB ensures that its practices are as efficient and flex¬ible as possible to achieve the highest level of cooperation between its members. It achieves this by using new technologies to keep working methods up to date, to minimise formalities and to provide efficient ad¬ministrative support;
- **Proactivity.** The EDPB anticipates and supports innovative solutions to overcome digital challenges to data pro¬tection. The EDPB encourages close collaboration with stakeholders (whether members, observers, staff or invited experts), so that their needs and aspira¬tions can be fully considered in its work.



3

2020 – Highlights

3.1. CONTRIBUTION OF THE EDPB TO THE EVALUATION OF THE GDPR

In February 2020, the EDPB and national Supervisory Authorities (SAs) contributed to the European Commission's evaluation and review of the GDPR, as required by Art. 97 GDPR.

The EDPB considers that the GDPR has strengthened data protection as a fundamental right and harmonised the interpretation of data protection principles. Data subject rights have been reinforced and data subjects are increasingly aware of the modalities to exercise their data protection rights. The GDPR also contributes to an increased global visibility of the EU legal framework and is being considered a role model outside of the EU. The EDPB believes that the GDPR's application have been successful, but acknowledges that a number of challenges still remain. For example, insufficient resources for SAs are still a concern, as are inconsistencies in national procedures that have an impact on the cooperation mechanism between SAs.

Despite these challenges, the EDPB is convinced that ongoing cooperation between SAs will facilitate a common data protection culture and establish consistent practices.

Furthermore, the EDPB believes it is premature to revise the GDPR.

3.2. ISSUES RELATING TO COVID-19 RESPONSES

During the COVID-19 pandemic, EEA Member States began taking measures to monitor, contain and mitigate the spread of the virus. Many of these measures involved the processing of personal data, such as contact-tracing apps, the use of location data or the processing of health data for research purposes. As such, the EDPB offered guidance on how to process personal data in the context of the COVID-19 pandemic.

3.2.1. Statement on the processing of personal data in the context of the COVID-19 outbreak

The EDPB emphasises that respecting data protection rules does not hinder the fight against the COVID-19 pandemic. Even in exceptional times, controllers and processors must ensure the protection of personal data.

The GDPR allows controllers to rely on several legal grounds for lawfulness of processing and enables competent public authorities and employers to lawfully process personal data in the context of a pandemic, in accordance with national law and the conditions set therein.

All measures implemented to manage the emergency should consider data protection principles, including purpose limitation, transparency, integrity and confidentiality.

When it comes to the use of mobile location data, the EDPB stresses that public authorities should first seek to process anonymous data, to which the GDPR does not apply. When this is not possible, national legislative measures safeguarding public security can be enacted by Member States, putting in place adequate safeguards (ePrivacy Directive). The proportionality principle should also guide public authorities in the use of mobile location data. This foregrounds anonymous solutions over intrusive measures, such as the "tracking" of individuals, which are proportional under exceptional circumstances and need to be subject to enhanced scrutiny to ensure the respect of data protection principles. The data minimisation principle should guide employers in the request and disclosure of health information in the context of COVID-19, meaning the least possible information should be disclosed to achieve a stated purpose.

Adopted: 20 March 2020

3.2.2. EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic

In its draft Guidance on apps supporting the fight against the COVID-19 pandemic, the European Commission proposed the development of a pan-European and coordinated approach in the use of such tools. The EDPB welcomes this initiative, recognising that no one-size-fits-all solution applies. SAs must be consulted during the elaboration and implementation of these measures to ensure that personal data is processed lawfully and respects individuals' rights.

Addressing specifically the use of apps for contact-tracing and warning individuals, the EDPB strongly supports the European Commission's proposal for the voluntary adoption of such apps to foster individual trust. This does not mean that personal data processing in this context must rely on an individual's consent, since other legal bases are available to public authorities. Contact-tracing apps should be able to discover events (i.e. contacts with COVID-19-positive people) without requiring location tracking of individual users. Both a so-called centralised and a so-called decentralised approach could be possible, provided that adequate security measures are in place.

Fully automated processes should be avoided through the strict supervision of qualified personnel, limiting the occurrence of false positives and negatives, and forms of stigmatisation.

Adopted: 14 April 2020

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

The GDPR's provisions that allow the processing of personal data for the purpose of scientific research are applicable also in the context of the COVID-19 pandemic. The Guidelines address urgent legal questions on the processing of health data for scientific research in the context of the pandemic. They address the following issues:

- **Legal basis.** Researchers should be aware that if explicit consent is used as the lawful basis for processing, all the conditions in Arts. 4(11), 6(1)(a), 7 and 9(2)(a) GDPR must be fulfilled. National legislators may enact specific laws to enable the processing of health data for scientific research purposes, pursuant to Arts. 6(1)(e) or (f) GDPR in combination with Arts. 9(2)(i) or (j) GDPR;
- **Data protection principles.** Considering the processing risks in the context of the COVID-19 outbreak, strong emphasis must be placed on the integrity and confidentiality of the data, the security of the processing, and the appropriate safeguards for the rights and freedoms of the data subject. It should be assessed whether a Data Protection Impact Assessment must be carried out;
- **Data subject rights.** Exceptional situations, such as the COVID-19 outbreak, do not suspend or restrict the possibility for data subjects to exercise their rights. The national legislator may allow restrictions to the data subject rights only in so far as it is strictly necessary.

Adopted: 21 April 2020

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

The EDPB believes that when processing personal data is necessary for implementing data-driven solutions in response to the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability, and guarantee the effectiveness of these solutions. The EDPB clarifies the conditions and principles for the proportionate use of the following:

- **Location data.** The ePrivacy Directive contains specific rules allowing for the collection of location data from both electronic communication providers and the terminal equipment. Preference should be given to processing anonymised location data;
- **Contact-tracing apps.** The development of such tools should give careful consideration to the principle of data minimisation and data protection by design and by default, for example by collecting only relevant information when absolutely necessary. Data broadcasted by the apps must only include some unique and pseudonymous identifiers, generated by and specific to the application.

The EDPB provides non-exhaustive recommendations and obligations to designers and implementers of contact-tracing apps to guarantee the protection of personal data from the early design stage.

Adopted: 21 April 2020

3.2.5. Statement on restrictions on data subject rights in connection to the state of emergency in Member States

When EEA Member States enter a state of emergency, such as the one brought on by the COVID-19 outbreak, the GDPR remains applicable and allows for efficient emergency response while protecting fundamental rights and freedoms.

Even in these exceptional times, the protection of personal data must be upheld in all emergency measures, including restrictions adopted at a national level. Art. 23 GDPR allows national legislators to restrict under specific circumstances the scope of some of the obligations and rights provided in the GDPR, as long as the restriction respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, inter alia, important objectives of general public interest.

Any restriction on a right must respect the essence of that right and thus cannot be as intrusive as to void fundamental rights of their basic content.

Further, restrictions need to be introduced by way of a legislative measure, as any limitation on the exercise of the rights and freedoms recognised by the EU Charter of Fundamental Rights must be "provided for by law". In particular, the domestic law must be sufficiently clear, and give an adequate indication of the circumstances in and conditions under which data controllers are empowered to resort to any such restrictions.

Legislative measures that seek to restrict the scope of data subject rights must be foreseeable to the people subject to them, including with regard to their duration in time. The restrictions need to genuinely pursue an important objective of general public interest of the EU or a Member State, such as public health. Data subject rights can be restricted, but not denied.

All restrictions on data subject rights must apply only in so far as it is strictly necessary and proportionate to safeguard the general public interest objective. The restrictions need to be limited in scope and in time, and cannot suspend or postpone the application of data subject rights and the obligations of data controllers and processors without any clear limitation in time, as this would equate to a de facto blanket suspension of those rights.

National authorities contemplating restrictions under Art. 23 GDPR should consult national SAs in due time.

Adopted: 2 June 2020

3.2.6. Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak

During the COVID-19 pandemic, many EEA Member States placed restrictions on freedom of movement within the internal market and Schengen area to mitigate the spread of the virus. On 15 June 2020, some Member States began to progressively lift these restrictions and re-open borders. In part, this was made possible by processing personal data at border crossings by, for example, administering COVID-19 tests or requesting health certificates.

The EDPB urges Member States to adopt a standardised approach to the processing of personal data in this context, emphasising that processing must be necessary and proportionate, and the measures should be based on scientific evidence. The EDPB highlights particular data protection principles to which Member States should pay special attention. It stresses the importance of prior consultation with competent SAs when Member States process personal data in this context.

Adopted: 16 June 2020

3.2.7. Statement on the data protection impact of the interoperability of contract tracing apps

The EDPB maintains that, without a common EEA approach in response to the COVID-19 pandemic, at least an interoperable framework should be put in place. The EDPB elaborates on the impact on the right to data protection that an interoperable implementation of contract tracing applications can entail by focusing on seven key areas:

- **Transparency.** Information on any additional personal data processing must be provided in clear and plain language to the data subject;
- **Legal basis.** Different legal bases used by different data controllers might require implementing additional measures to safeguard data subject rights related to the legal basis;
- **Controllership.** Any operations that ensure interoperability should be considered separate to prior or subsequent processing for which the parties are individual controllers or joint controllers;
- **Data subject rights.** The exercise of rights should not become more cumbersome for the data subjects;
- **Data retention and minimisation.** Common levels of data minimisation and data retention periods should be considered;
- **Information security.** Providers should consider the additional information security risk caused by the additional processing;
- **Data accuracy.** Measures should be put in place to ensure data accuracy is maintained in the interoperable system.

Adopted: 16 June 2020

3.2.8. EDPB response Letters on COVID-related matters

During the COVID-19 pandemic, the EDPB responded to letters from different stakeholders asking for further clarifications on COVID-19-related matters. The EDPB received letters from the following parties: public officials (including Members of the European Parliament Ďuriš Nicholsonová and Sophie in 't Veld, and the United States Mission to the European Union); civil liberties advocacy organisations (Civil Liberties Union for Europe, Access Now and the Hungarian Civil Liberties Union); and private companies (Amazon EU Sarl).

In its responses, the EDPB reiterated that data protection legislation already takes into account data processing operations that are necessary to contribute to the fight against the pandemic, and that the data protection principles need always to be upheld. Where relevant, the EDPB referred to published or future Guidelines addressing the matters in question or encouraged consultation with national SAs.

Adopted: 24 April 2020, 19 May 2020, 3 June 2020, 17 July 2020

3.3. INTERNATIONAL PERSONAL DATA FLOWS AFTER THE *SCHREMS II* JUDGMENT

On 16 July 2020, the Court of Justice of the EU (CJEU) released its judgment in Case C-311/18 (*Schrems II*). The CJEU examined two mechanisms that allow personal data transfers from the EEA to non-EEA countries (third countries), namely, the EU-U.S. Privacy Shield and Standard Contractual Clauses (SCCs). The CJEU invalidated the adequacy decision underlying the EU-U.S. Privacy Shield, thereby rendering it invalid as a transfer mechanism. It also ruled that the European Commission's Decision 2010/87 on SCCs for the transfer of personal data to third country processors is valid, so SCCs may still be used to

enable international data transfers. This is upon the condition that the exporter (if needed, with the help of the importer), assesses, prior to the transfer, the level of protection afforded in the context of such transfers, taking into consideration both the SCCs and the relevant aspects of the legal system of the importer's country, as regards any access to the data by that third country's public authorities. The factors to be considered for this assessment are those set out, in a non-exhaustive manner, in Art. 45(2) GDPR.

The judgment has wide-ranging implications for EEA-based entities that use these mechanisms to enable personal data transfers to the U.S. and other third countries.

3.3.1. Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems

The EDPB believes that the CJEU's judgment in Case C-311/18 (*Schrems II*) highlights the importance of the fundamental right to privacy in the context of the transfer of personal data to third countries and the risk for data subjects caused by possible indiscriminate access by a third country's public authorities to the personal data transferred. Standard Contractual Clauses (SCCs) must maintain a level of protection in the third country that is essentially equivalent to that in the EEA.

The EDPB notes that the judgment emphasises that the assessment of whether the SCCs can ensure in practice for the data transferred to a third country an essentially equivalent level of protection is primarily the responsibility of exporters and importers. If the SCCs by themselves cannot guarantee an essentially equivalent level of protection in the third country, the exporter will need to consider putting in place supplementary measures that fill the protection gap.

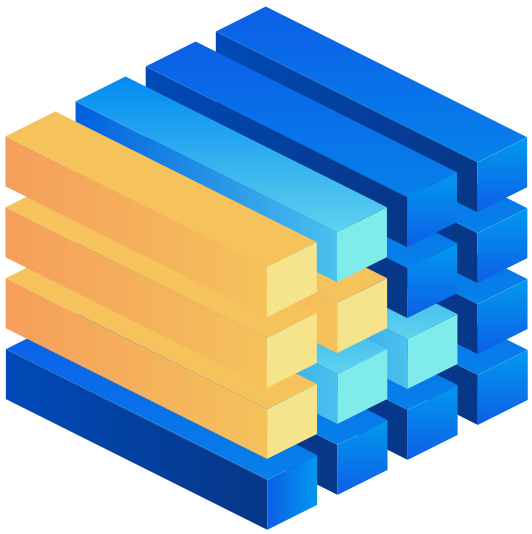
The judgment recalls and the EDPB underlines that the exporter and the importer need to comply with their obligations included in the SCCs. If they do not or cannot comply with these obligations, the exporter must suspend the transfer or terminate the agreement.

The EDPB notes that competent SAs have the duty to suspend or prohibit a personal data transfer to a third country pursuant to SCCs if they are not or cannot be complied with in that third country, and the protection of the data transferred cannot be ensured by other means, in particular where the exporter or importer has not already itself suspended or put an end to the transfer.

The EDPB recalls its position on the use of the derogations under Art. 49 GDPR, as set out in its Guidelines 02/2018, which must be applied on a case-by-case basis.

The EDPB will keep assessing the judgment and will continue providing guidance on its consequences for personal data transfers to countries outside the EEA. .

Adopted: 17 July 2020



3.3.2. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

Following the CJEU's judgment in Case C-311/18 (*Schrems II*), the EDPB provided clarifications on the judgment in a document addressing 12 Frequently Asked Questions (FAQs).

These answers stipulated that:

- There is no grace period for EEA organisations relying on the Privacy Shield to transfer personal data to the U.S.;
- As a consequence, any personal data transfers from the EEA to the U.S. are illegal if they are based on the Privacy Shield;
- The threshold set by the CJEU for transfers to the U.S. applies for any third country;
- Therefore, the CJEU's approach applies to any international data transfers relying on SCCs and, by extension, those relying on Binding Corporate Rules (BCRs) or on other Art. 46 GDPR transfer mechanisms;
- Whether or not personal data may be transferred to a third country on the basis of an Art. 46 GDPR transfer mechanism depends on the outcome of the prior assessment to be carried out by the exporter, taking into account the specific circumstances of the transfers, and the supplementary measures possibly identified. The transfer mechanism used and the supplementary measures would have to ensure that the laws of the third country of destination do not impinge on the adequate level of protection guaranteed by such mechanisms and supplementary measures;
- It is still possible to transfer personal data from the EEA to the U.S. on the basis of derogations under Art. 49 GDPR, provided the conditions set forth in this provision apply. On this provision, the EDPB refers to its Guidelines 02/2018.

SAs will cooperate within the EDPB to ensure consistency, in particular if transfers to third countries must be prohibited.

Adopted: 23 July 2020

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

The CJEU mentioned in its judgment in Case C-311/18 (*Schrems II)* the possibility for exporters of adopting supplementary measures to bring the level of protection of personal data transferred to countries outside the EEA up to the standard of essential equivalence with the EU level, where Art. 46 GDPR transfer tools cannot guarantee it by themselves. The EDPB issued Recommendations that provide data exporters with a series of six steps to follow to apply the principle of accountability to data transfers, and some examples of supplementary measures.

These steps addressed to data exporters are as follows:

- Step 1: Data exporters should know their transfers in order to be fully aware of the destination of the personal data processing and verify that personal data is adequate, relevant and limited to what is necessary in relation to the purpose for which it is transferred.
- Step 2: Data exporters should identify the transfer tools under Chapter V GDPR, which they are relying on. Relying on some tools, such as a valid adequacy decision covering the third country, will be enough to proceed with the transfer without taking any further steps, other than monitoring that the decision remains valid.

- Step 3: Data exporters should assess the laws and/or practices of the third country to determine if these could impinge on the effectiveness of the safeguards contained in the transfer tools the data exporter is relying on. This assessment should be primarily focused on third country legislation relevant to the transfer and the transfer tool relied on that could undermine its level of protection and other objective factors. The EDPB Recommendations 02/2020 on the European Essential Guarantees will be relevant in this context to evaluate the third country legislation on public authorities' access for the purpose of surveillance.
- Step 4: Data exporters should identify and adopt supplementary measures, such as various technical, contractual and organisational measures to bring the level of protection of the data transferred up to the EU standard of essential equivalence. The EDPB Recommendations 01/2020 contain in their Annex a non-exhaustive list of examples of supplementary measures with some of the conditions they would require to be effective. Data exporters must avoid, suspend or terminate the transfer to avoid compromising the level of protection of the personal data in those cases where they find no suitable supplementary measures. Data exporters should also conduct the assessment with due diligence and document it.
- Step 5: Where required, data exporters should take formal procedural steps, such as consulting competent SAs.
- Step 6: Data exporters should re-evaluate the level of protection afforded to personal data at appropriate intervals, in accordance with the principle of accountability.

Adopted: 10 November 2020

3.3.4. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

In light of the CJEU's judgment in Case C-311/18 (*Schrems II*), the EDPB updated the Recommendations on the European Essential Guarantees (EEG) for surveillance measures.

The Recommendations are based on the jurisprudence of the CJEU and the European Court of Human Rights. The case law from these Courts reasserts that public authorities' access, retention and further use of personal data through surveillance measures must be limited to what is strictly necessary and proportionate in a democratic society.

The Recommendations describe four EEG. The EEG are the core elements to be found when assessing the level of interference with the fundamental rights to privacy and data protection of the surveillance measures conducted by public authorities in third countries. The EEG are also part of the assessment that data exporters need to conduct to determine if a third country provides a level of protection essentially equivalent to that guaranteed within the EEA.

The EEG as updated by the Recommendations are as follows:

- Processing should be based on clear, precise and accessible rules;
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;
- An independent oversight mechanism should exist;
- Effective remedies need to be available to the individual. These include providing data subjects with the possibility of bringing legal action before an independent and impartial court or body to have access to their personal data or to obtain the rectification or erasure of such data;
- A notification to the individual whose personal data has been collected or analysed must occur only to the extent that and as soon as it no longer jeopardises the tasks of public authorities.

The EEG should be assessed on an overall basis, as they are closely interlinked. These guarantees require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework.

The assessment of third country surveillance measures may lead to one of two conclusions:

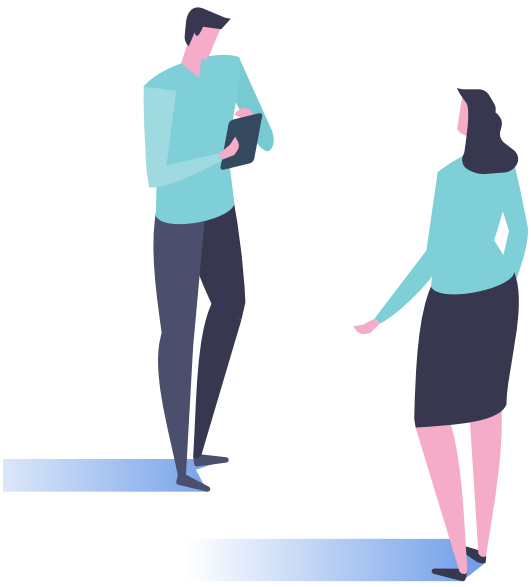
- The third country legislation at issue does not ensure the EEG requirements and thus does not provide a level of protection essentially equivalent to that guaranteed within the EEA; or
- The third country legislation at issue satisfies the EEGs.

Adopted: 10 November 2020

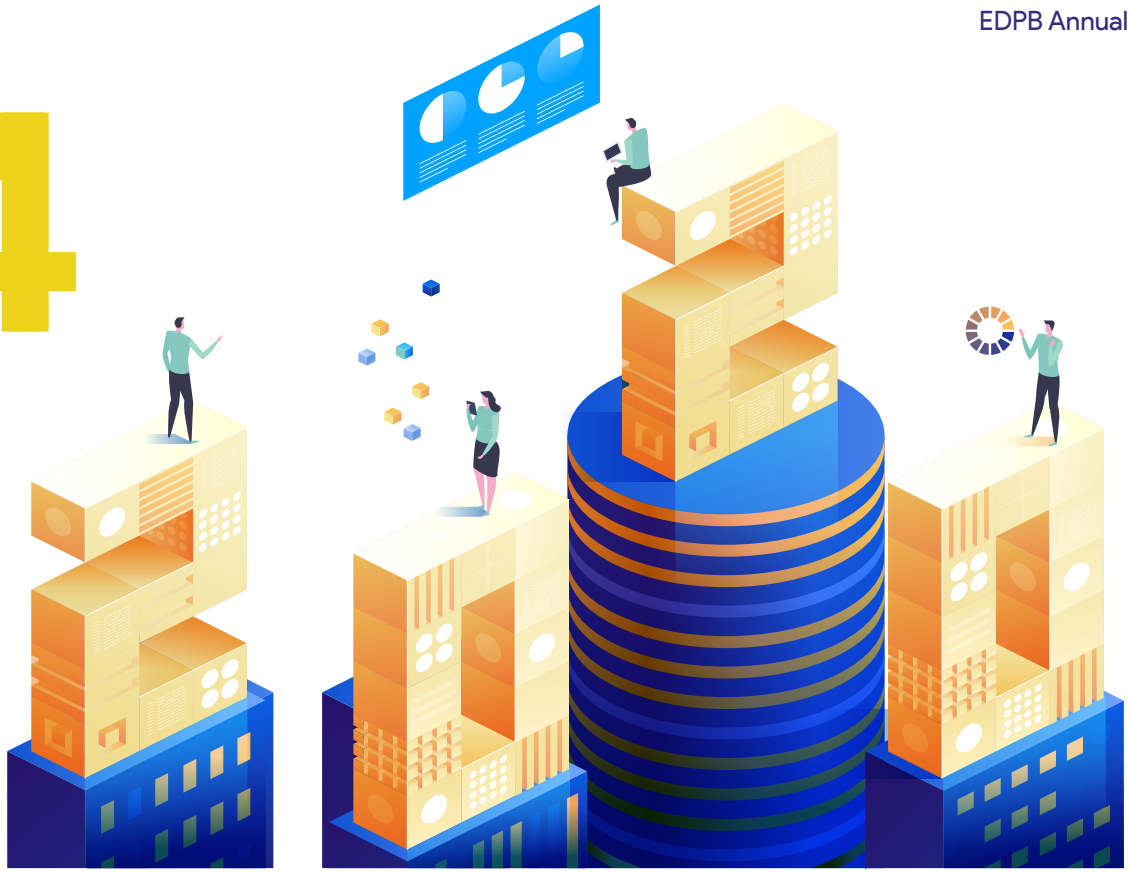
3.4. FIRST ART. 65 GDPR BINDING DECISION

The EDPB adopted its first dispute resolution decision on the basis of Art. 65 GDPR. The binding decision addressed the dispute that arose after the Irish SA, acting as Lead SA, issued a draft decision regarding Twitter International Company and the subsequent relevant and reasoned objections expressed by a number of Concerned SAs. Section 5.3 of this Report further elaborates upon this decision.

Adopted: 9 November 2020



4



2020 - An overview

4.1. FUNCTIONING OF THE EDPB: REVISED RULES OF PROCEDURE

During its first plenary meeting on 25 May 2018, the EDPB adopted its Rules of Procedure (RoP), which outline the EDPB's primary operational rules, including:

- The EDPB's guiding principles;
- The EDPB's organisational framework;
- The cooperation between EDPB Members;
- The election of the Chair and Deputy Chair of the EDPB;
- The EDPB's working methods.

In January 2020, the EDPB adopted revisions to Arts. 10(1), 10(2) and 10(5) RoP and in October 2020, it adopted an amendment to Art. 11(2) RoP.

4.2. THE EDPB SECRETARIAT

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

Although staff at the EDPB Secretariat are employed by the EDPS, staff members only work under the instructions of the Chair of the EDPB. A Memorandum of Understanding establishes the terms of cooperation between the EDPB and the EDPS.

In 2020, due to limitations brought on by the COVID-19 pandemic, the EDPB Secretariat implemented novel measures to improve working conditions amidst unprecedented circumstances. These measures included: employing new videoconferencing tools; holding more frequent meetings; and implementing new initiatives to keep the EDPB Members connected, for example the addition of extra Jabber accounts and a new Wiki platform.

In light of these circumstances, the EDPB Secretariat organised a substantially increased number of EDPB meetings in 2020. The EDPB held 172 meetings, including plenary meetings and expert subgroup meetings, where ordinarily they would hold about 100 meetings. Notably, the EDPB held 27 plenary meetings, compared to 11 in previous years.

The EDPB Secretariat also led the drafting of over 60% of the Guidelines, Opinions, Recommendations and Statements adopted by the EDPB in 2020.

The EDPB designated a DPO in accordance with Art. 43 Regulation 2018/1725. The DPO's position and tasks are defined in Arts. 44 and 45 of said Regulation, and are further detailed in the EDPB DPO Implementing Rules.

4.3. COOPERATION AND CONSISTENCY

As stated in the GDPR, the SAs of EEA Member States cooperate closely to ensure that people's data protection rights are protected consistently across the EEA. They assist each other and coordinate their decision-making in cross-border data protection cases.

Through the so-called consistency mechanism, the EDPB issues Consistency Findings, comprising Opinions and Decisions (outlined in Chapter 5 of this Report), to clarify fundamental provisions of the GDPR and to ensure consistency in its application among SAs.

In 2020, the EDPB issued 32 Opinions under Art. 64 GDPR. Most of these Opinions concern draft accreditation requirements for a code of conduct monitoring body or a certification body, as well as Controller Binding Corporate Rules for various companies.

In November 2020, the EDPB adopted its first dispute resolution decision on the basis of Art. 65 GDPR to address a dispute that arose after the Irish SA, acting as Lead SA, issued a draft decision regarding Twitter International Company and the subsequent relevant and reasoned objections expressed by a number of Concerned SAs.

The EDPB also published a register of decisions taken by national SAs in line with the One-Stop-Shop cooperation procedure (Art. 60 GDPR) on its website.

In November 2020, the EDPB adopted a document on the procedure for the development of informal "Codes of Conduct sessions", in which it proposes a format for the Codes sessions. The document further elaborates on the role of SAs, and their interaction with both the competent SAs and the Code owners, as well as on the role of the EDPB Secretariat.

With increasing attention placed on the cooperation mechanism outlined in the GDPR, the EDPB in October 2020 issued Guidelines to establish a common understanding of the notion of a "relevant and reasoned" objection and to address any unfamiliarity surrounding its interpretation.

In October 2020, the EDPB released a document on the Coordinated Enforcement Framework (CEF), which provides a structure for coordinating recurring annual activities by SAs. The main objective of the CEF is to facilitate joint actions in a flexible but coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations.

As part of its 2021-2023 Strategy, the EDPB decided to establish a Support Pool of Experts (SPE) on the basis of a pilot project. The goal is to provide material support to EDPB Members in the form of expertise that is useful for investigations and enforcement activities, and to enhance cooperation and solidarity between EDPB Members by sharing, reinforcing and complementing strengths and addressing operational needs. In December 2020, the EDPB adopted a document on the terms of reference of the SPE.

In July 2020, the EDPB adopted an information note with regard to arrangements to be made by BCR holders with the United Kingdom SA (UK SA) as the competent SA (BCR Lead SAs). In light of Brexit, BCR Lead SAs need to make all organisational arrangements to establish a new BCR Lead in the EEA. In December 2020, the EDPB issued a statement on the end of the Brexit transition period in which it describes the main implications of the end of this period for data controllers and processors. In particular, the EDPB underlines the issue of data transfers to a third country as well as the consequences in the area of regulatory oversight and the One-Stop-Shop mechanism. The Brexit transition period, during which the UK SA was still involved in the EDPB's administrative cooperation, expired at the end of 2020. Additionally, the EDPB adopted an information note on data transfers under the GDPR after the Brexit transition period ends.

4.3.1. IT communications tool (Internal Market Information system)

The EDPB promotes the cooperation between SAs by providing a robust IT system. Since 25 May 2018, SAs have been using the Internal Market Information (IMI) system to exchange information necessary for the GDPR cooperation and consistency mechanism in a standardised and secured way.

The European Commission's Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) developed the IMI system. In the context of the EDPB, it was adapted in close cooperation with the EDPB Secretariat and SAs to cater to the needs of the GDPR. Since its implementation, the IMI system has proven to be an asset for SAs, which continue to use and access the system daily.

In 2020, SAs registered 628 cases in the IMI system.[1] They also initiated a number of procedures in the same period, described below:

- Identification of the Lead SA and Concerned SAs: 742 procedures;
- Mutual Assistance Procedures: 246 formal procedures and 2,258 informal procedures;
- One-Stop-Shop mechanism – draft decisions and final decisions: 203 draft decisions, from which 93 resulted in final decisions.

1. A case entry refers to an entry in the IMI system that allows the management of cooperation or consistency procedures from beginning to end. It is a central point where SAs can share and find information on a specific issue to facilitate the retrieval of information and the consistent application of the GDPR.

A case entry may consist of the management of multiple procedures (e.g. an Art. 60 GDPR procedure or an Art. 65 GDPR procedure in case of disagreement) or just a single one related to a case register entry. Multiple complaints on the same subject relating to the same processing can be bundled in one single case entry.

5

European Data Protection Board Activities in 2020

To ensure the consistent application of the GDPR across the EEA, the EDPB issues general guidance to clarify European data protection laws.

This guidance provides the public and stakeholders with a consistent interpretation of their rights and obligations, and ensures that national Supervisory Authorities (SAs) have a benchmark for applying and enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Binding Decisions to guarantee the consistent application of the GDPR by SAs. Throughout 2020, the EDPB issued multiple guidance and consistency documents, as summarised below.

5.1. GENERAL GUIDANCE (GUIDELINES, RECOMMENDATIONS, BEST PRACTICES)

In 2020, the EDPB adopted several Guidelines and Recommendations on the data protection requirements pertaining to the COVID-19 pandemic (see Section 3.2 of this Report), new technologies, personal data transfers and the meaning of specific terms in the GDPR.

These Guidelines and Recommendations are summarised below.

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

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

The EDPB Guidelines aim to clarify the key privacy and data protection risks, including the security of personal data, ensuring full control over processing, and the appropriate legal basis for further processing and how GDPR-compliant consent should be collected in cases of multiple processing.

In order to mitigate the risks to data subjects, the EDPB identifies three categories of personal data requiring special attention:

- Location data, which, due to its sensitive nature, should not be collected except if doing so is absolutely necessary for the purpose of processing;
- Biometric data, which should be stored locally and in encrypted form;
- Data revealing criminal offences and other infractions, the processing of which is subject to the safeguards contained in Art. 10 GDPR.

The EDPB also highlights the interplay between the GDPR and the ePrivacy Directive, noting that the connected vehicle and any device connected to it should be considered "terminal equipment" for the purposes of Art. 5(3) ePrivacy Directive.

Adopted: 28 January 2020

5.1.2. Guidelines 02/2020 on Arts. 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies

In its Guidelines, the EDPB provides guidance on the transfers of personal data from EEA public bodies to public bodies in third countries, or to international organisations, for the purpose of various administrative cooperation endeavours that fall within the scope of the GDPR.

The EDPB outlines general recommendations for additional appropriate safeguards to be adopted by public bodies for the transfer of personal data and notes the core data protection principles that are to be ensured by the parties to a transfer. Public bodies may implement appropriate safeguards either through a legally binding and enforceable instrument under Art. 46(2)(a) GDPR, or through provisions to be inserted into administrative arrangements under Art. 46(3)(b) GDPR.

The EDPB notes that any international agreement concluded between EEA and non-EEA public authorities should also safeguard data subject rights and provide for a redress mechanism that enables data subjects to exercise their rights in practice.

Adopted: 15 December 2020

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

See Section 3.2.3 for a full summary.

The GDPR's provisions on personal data processing for scientific research are also applicable in the context of the COVID-19 pandemic.

The EDPB Guidelines address key questions on the processing of health data for scientific research in the context of the pandemic.

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

See Section 3.2.4 for a full summary.

When processing personal data is necessary for implementing data-driven solutions in response to the COVID-19 pandemic, data protection is key to ensuring effective solutions, which are socially accepted. The EDPB clarifies the conditions and principles for the proportionate use of location data and contact-tracing apps.

5.1.5. Guidelines 05/2020 on consent under Regulation 2016/679

Over the last decade, the Article 29 Working Party and the EDPB have issued guidance on consent as a legal basis for personal data processing. Past guidance has focused on defining valid consent as "freely given", "specific", "informed" and "unambiguous".

The EDPB updated the Article 29 Working Party guidance to avoid misinterpretation and to further clarify the meaning of consent with regard to personal data processing in the areas of cookie walls and user actions, such as scrolling or swiping. In this context, data controllers must ensure the following:

- Cookie walls must give users clear and equal options to accept or reject cookies;
- Cookie walls must allow users to access content without clicking "Accept Cookies". If content is inaccessible without making a choice about cookies, the user is not given a genuine choice and consent is therefore not "freely given";
- Actions such as scrolling or swiping through a webpage do not constitute a clear and affirmative action needed for lawful consent;
- Consent must be as easy to withdraw as it is to provide.

Adopted: 4 May 2020

5.1.6. Guidelines 06/2020 on the interplay with the Second Payments Services Directive and the GDPR

The second Payments Services Directive (PSD2) repeals Directive 2007/64/EC and provides legal clarity for entities involved in the provision of payment services within the EEA.

The Guidelines are a more detailed and considered response, requested to support an initial letter, concerning regulatory

interplay between the GDPR and the PSD2. The Guidelines provide clarification on aspects related to the collection and processing of personal data by entities involved in the payments services sector. More specifically, the PSD2 provides clarity to those data controllers that have legal obligations associated with the PSD2. The EDPB confirms that controllers in the payment services sector should always ensure compliance with the requirements of the GDPR and stresses this importance. The EDPB, however, is appreciative of the regulatory uncertainty given the complexity of the interplay between the GDPR and the PSD2.

The Guidelines focus on a number of components critical to the interplay between the two legal frameworks. In summary, they provide guidance and clarity on the following subjects:

- Lawful grounds and further processing;
- Explicit consent;
- The processing of silent party data;
- The processing of special categories of data under the PSD2;
- Data minimisation, security, transparency, accountability and profiling.

Adopted: 17 July 2020

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

This updated EDPB guidance builds upon and replaces the Article 29 Working Party Opinion 01/2010 (WP169) on the concepts of "controller" and "processor", providing more developed and specific clarifications of these concepts in light of the changes brought by the GDPR.

The Guidelines offer a focus on definitions and pragmatic consequences attached to the different data protection roles, clarifying the following concepts:

- The concepts of controller, joint controller and processor are functional and autonomous concepts: they allocate responsibilities according to the actual roles of the parties and they should be interpreted mainly according to EU data protection law.
- The data controller may be defined by law or may be established on the basis of an assessment of the factual circumstances surrounding the processing. Controllers are the ones that determine both purposes and "means" of the processing, i.e. the "why" and the "how";
- The data processor processes personal data on behalf of the controller and must not process the data other than according to the controller's instructions, but the processor may be left a certain degree of discretion and may determine more practical aspects of the processing, including "non-essential means". Data processing agreements between controllers and processors should include specific and concrete information on how the requirements set out by Art. 28 GDPR will be met;
- Joint controllers are two or more entities that jointly determine the purposes and means of the processing through "common decisions" or "converging decisions", in such a manner that the processing by each party is inseparable. The distribution and allocation of obligations among joint controllers can have a degree of flexibility, as each controller shall ensure its processing is carried out in compliance with data protection requirements. Although the legal form of the arrangement among joint controllers is not specified by the GDPR, the EDPB recommends that it should be made in the form of a binding document.

Adopted: 2 September 2020

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

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

Within this environment, the EDPB identifies three key actors:

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

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

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

Adopted: 2 September 2020

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

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

Under the cooperation mechanism, and specifically under Art. 60(3) GDPR, a Lead Supervisory Authority (LSA) is required to submit a draft decision to the Concerned Supervisory Authorities (CSAs), who may then raise a "relevant and reasoned objective" within the set timeframe.

In this context, the EDPB further clarifies the meaning of each of the elements of the definition in Art. 4(24) GDPR, which requires a relevant and reasoned objection to determine whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR, and to clearly demonstrate the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the EU.

The EDPB notes that for an objection to be "relevant", there should be a direct connection between the draft decision at hand and the objection, since the objection, if followed, would entail a change to the draft decision leading to a different conclusion as to whether there is an infringement of the GDPR, or whether the envisaged action towards the controller or processor complies with the GDPR.

The objection will be "reasoned" when it is clear, precise, coherent and detailed in explaining the reasons for objection, through legal or factual arguments. The EDPB also provides clarifications on the obligation for the CSAs to clearly demonstrate in their objection the significance of the risks

posed by the draft decision for the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data.

Adopted: 8 October 2020

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

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

Under specific conditions, Art. 23 GDPR allows a national or EEA legislator to restrict, by way of a legislative measure, the scope of the rights and obligations enshrined in Chapter III GDPR (data subject rights) and corresponding provisions of Art. 5 GDPR, as well as Art. 34 GDPR, only if this restriction respects the essence of the relevant fundamental rights and freedoms, and is a necessary and proportionate measure in a democratic society to safeguard, amongst others, national security or important objectives of general public interest. The legislator issuing the legislative measures that set out the restrictions and the data controllers applying them should be aware of the exceptional nature of these restrictions.

The Guidelines provide details on the interpretation of each of these requirements, also highlighting how the requirement for a legislative measure can be met and the fact that such a measure needs to be adapted to the objective pursued. It also needs to meet the foreseeability criterion by being sufficiently clear so as to give individuals an adequate indication of the circumstances in which controllers are empowered to resort to restrictions.

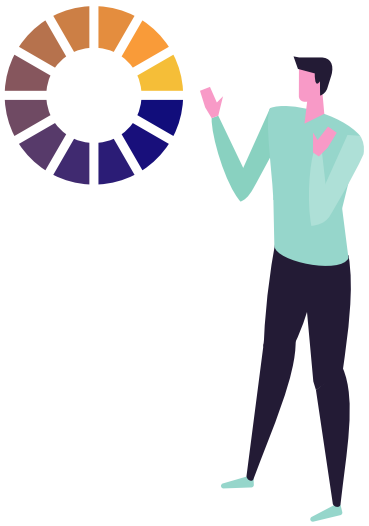
Restrictions under Art. 23 GDPR need to pass a necessity and proportionality test, typically implying the assessment of risks to the rights and freedoms of data subjects. The necessity test is based on the objective of general interest pursued. Only where the necessity test is satisfied, the proportionality of the measure is assessed.

The Guidelines also provide information concerning the specific requirements set out in Art. 23(2) GDPR, whereby the legislative measures setting out the restrictions need to contain specific provisions concerning a list of elements, including the purposes of processing, the scope of the restrictions, and the risks to the rights and freedoms of data subjects.

The controller should document the application of restrictions to concrete cases in line with the accountability principle and should lift the restrictions as soon as the circumstances that justify them no longer apply. Once restrictions are lifted, data subjects must be allowed to exercise all their rights in relation to the data controller.

SAs should be consulted before the adoption of the legislative measures setting the restrictions and have the powers to enforce compliance with the GDPR.

Adopted: 15 December 2020



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

See Section 3.3.3 for the full summary.

With these Recommendations, the EDPB seeks to help data exporters comply with EU law governing international transfers, as clarified by the Court of Justice of the EU in its judgment in Case C-311/18 (*Schrems II*). The Recommendations provide data exporters with six steps to follow to ensure that the personal data transferred is afforded a level of protection essentially equivalent to that guaranteed within the EU. The Recommendations also describe several examples of supplementary measures that could in certain situations contribute to ensuring the protection of personal data required under EU law.

5.1.12. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

See Section 3.3.4 for the full summary.

These Recommendations update the content of a working document issued by the Article 29 Working Party with the clarifications that the Court of Justice of the EU and the European Court of Human Rights provided since the publication of this working document. The European Essential Guarantees describe four guarantees to be found when assessing the level of interference with the fundamental rights to privacy and data protection of surveillance measures in third countries.

5.1.13. Guidelines adopted following public consultation

5.1.13.1. Guidelines 03/2019 on processing personal data through video devices

The proliferation of video devices in many spheres of individuals' daily lives has considerable implications for data protection and privacy. The use of facial recognition and analysis software could threaten to reinforce society's problematic prejudices, and systematic video surveillance could lead to an acceptance of the lack of privacy as the default.

In its Guidelines, the EDPB notes that the most likely legal bases for processing video surveillance data are legitimate interest under Art. 6(1)(f) GDPR and consent under Art. 6(1)(e) GDPR. When relying on legitimate interest as the legal basis, the necessity of deploying video surveillance needs to be proven, and a balancing test needs to be carried out on a case-by-case basis. When relying on consent, the EDPB recalls that it shall be "freely given, specific, informed and unambiguous".

The Guidelines highlight the need to pay particular attention to the processing of special categories of personal data, including biometric data. These could be identified when conducting a Data Protection Impact Assessment under Art. 35(1) GDPR, the results of which can inform the data protection measures that data controllers should implement.

The EDPB notes that the principle of transparency and the obligation to inform data subjects of video surveillance operations are crucial. The Guidelines elaborate on how controllers can fulfil these obligations and ensure that data subject rights can be exercised in practice.

Adopted: 29 January 2020

5.1.13.2. Guidelines 05/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)

The EDPB adopted the final version of its guidance with regards to the personal data processed by search engine providers and data subject requests for delisting.

The Guidelines provide insight into the six grounds on which to request delisting pursuant to Art. 17(1) GDPR, including when the personal data is no longer necessary in relation to its purposes, the data subject withdraws their consent, the personal data is otherwise unlawfully processed, or when the data subject exercises the right to object.

The EDPB also provided clarifications as to the exceptions to the right to request delisting as found in Art. 17(3) GDPR.

Adopted: 7 July 2020

5.1.13.3. Guidelines 04/2019 on Art. 25 GDPR Data Protection by Design and by Default Version 2.0

Art. 25 GDPR enshrines the principles of Data Protection by Design and by Default (DPbDD), which form a crucial part of personal data protection legislation and act as key obligations for data controllers. Whilst the Guidelines mainly address data controllers, other actors such as processors and designers of products and services will also benefit from them.

The EDPB notes that controllers have to implement DPbDD through appropriate technical and organisational measures early on, and integrate necessary safeguards into the processing throughout its lifecycle. These measures ensure that data subject rights and freedoms are protected, and that data protection principles are effectively implemented.

The Guidelines also provide a number of recommendations for how controllers, processors and third parties in the ecosystem may cooperate to achieve DPbDD. In particular, they may engage Data Protection Officers from the outset, train employees on basic "cyber hygiene" and rely on codes of conduct to demonstrate compliance.

Adopted: 20 October 2020

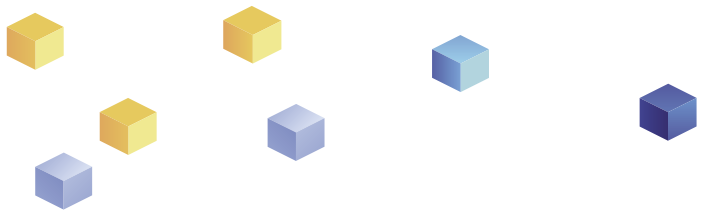
5.2. CONSISTENCY OPINIONS

The EDPB aims to ensure the consistent application of the GDPR across the EEA. To enable this, SAs from EEA countries must request an Opinion from the EDPB before adopting any decision in areas specified by the GDPR as having cross-border implications. This applies when an SA does the following:

- Intends to adopt a list of the processing operations subject to the requirement for a Data Protection Impact Assessment;
- Intends to adopt a draft code of conduct relating to processing activities;
- Aims to approve the criteria for accreditation of certification bodies;
- Aims to adopt Standard Contractual Clauses;
- Aims to approve Binding Corporate Rules.

The competent SA must take utmost account of the Opinion. The EDPB's Opinions pertaining to specific SAs and their implementation efforts are outlined below.

See Section 5.5.



5.2.1. Opinions on draft accreditation requirements for code of conduct monitoring bodies

The EDPB issued 11 Opinions on draft accreditation requirements for code of conduct monitoring bodies, as submitted by individual SAs. The SAs submitted their draft accreditation requirements and each requested an Opinion under Art. 64(1)(c) GDPR.

The aim of such EDPB Opinions is to ensure consistency and the correct application of the requirements among EEA SAs. In order to do so, the EDPB made several recommendations and encouragements to the various SAs on the amendments to be made to the draft accreditation requirements.

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

The various Opinions are listed below:

- Opinion 01/2020 on the Spanish data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 28 January 2020
- Opinion 02/2020 on the Belgium data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 28 January 2020
- Opinion 03/2020 on the France data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 28 January 2020
- Opinion 10/2020 on the draft decision of the competent Supervisory Authorities of Germany regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 25 May 2020
- Opinion 11/2020 on the draft decision of the competent Supervisory Authority of Ireland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 25 May 2020
- Opinion 12/2020 on the draft decision of the competent Supervisory Authority of Finland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 25 May 2020
- Opinion 13/2020 on the draft decision of the competent Supervisory Authority of Italy regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 25 May 2020
- Opinion 18/2020 on the draft decision of the competent Supervisory Authority of the Netherlands regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 July 2020
- Opinion 19/2020 on the draft decision of the competent Supervisory Authority of Denmark regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 July 2020
- Opinion 20/2020 on the draft decision of the competent Supervisory Authority of Greece regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 July 2020
- Opinion 31/2020 on the draft decision of the competent Supervisory Authority of Poland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 7 December 2020

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

Ten SAs individually submitted their draft decisions on accreditation requirements for certification bodies under Art. 43(1)(b) GDPR to the EDPB, requesting an Opinion under Art. 64(1)(c) GDPR. The accreditation requirements allow the relevant national accreditation body to accredit certification bodies responsible for issuing and renewing certification in accordance with Art. 42 GDPR.

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

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

The various Opinions are listed below:

- Opinion 04/2020 on the draft decision of the competent Supervisory Authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 GDPR Adopted: 29 January 2020
- Opinion 05/2020 on the draft decision of the competent Supervisory Authority of Luxembourg regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 29 January 2020
- Opinion 14/2020 on the draft decision of the competent Supervisory Authority of Ireland regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 25 May 2020
- Opinion 15/2020 on the draft decision of the competent Supervisory Authorities of Germany regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 25 May 2020
- Opinion 16/2020 on the draft decision of the competent Supervisory Authority of the Czech Republic regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 25 May 2020
- Opinion 21/2020 on the draft decision of the competent Supervisory Authority of the Netherlands regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 23 July 2020
- Opinion 22/2020 on the draft decision of the competent Supervisory Authority of Greece regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 23 July 2020
- Opinion 23/2020 on the draft decision of the competent Supervisory Authority of Italy regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 23 July 2020
- Opinion 26/2020 on the draft decision of the competent Supervisory Authority of Denmark regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 7 December 2020
- Opinion 30/2020 on the draft decision of the competent Supervisory Authority of Austria regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 7 December 2020

5.2.3. Opinions on draft decisions regarding Binding Corporate Rules

SAs may approve Binding Corporate Rules (BCRs) within the meaning of Art. 47 GDPR. BCRs are data protection policies implemented and adhered to within a group of enterprises established in the EEA for transfers of personal data outside the EEA within the same group.

In 2020, several SAs submitted their draft decisions regarding the Controller or Processor BCRs of various companies to the EDPB, requesting an Opinion under Art. 64(1)(f) GDPR. The EDPB issued nine Opinions on BCRs. In all instances, the EDPB concluded that the draft BCRs contained all required elements, and guaranteed appropriate safeguards to ensure that the level of protection in the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. They could therefore be adopted without changes.

The relevant SAs then went on to approve the BCRs.

The various Opinions are listed below:

- Opinion 06/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Fujikura Automotive Europe Group (FAE Group) Adopted: 29 January 2020
- Opinion 08/2020 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Reinsurance Group of America Adopted: 14 April 2020
- Opinion 09/2020 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of Reinsurance Group of America Adopted: 14 April 2020
- Opinion 24/2020 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of Jotun Adopted: 31 July 2020
- Opinion 25/2020 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Tetra Pak Adopted: 31 July 2020
- Opinion 27/2020 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Coloplast Group Adopted: 8 December 2020
- Opinion 28/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Iberdrola Group Adopted: 8 December 2020
- Opinion 29/2020 on the draft decision of the Lower Saxony Supervisory Authority regarding the Controller Binding Corporate Rules of Novelis Group Adopted: 8 December 2020
- Opinion 32/2020 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of Equinix Adopted: 15 December 2020

5.2.4. Other Opinions

Opinion 07/2020 on the draft list of the competent Supervisory Authority of France regarding the processing operations exempt from the requirement of a Data Protection Impact Assessment (Art. 35(5) GDPR) Adopted: 22 April 2020

Under Arts. 35(6) and 64(2) GDPR, the EDPB issues an Opinion where an SA intends to adopt a list of data processing operations not subject to the requirement for a Data Protection Impact Assessment pursuant to Art. 35(5) GDPR. The French Supervisory Authority (FR SA) submitted an update of its draft list of exempt processing activities to the EDPB for its consideration.

The EDPB clarified that 12 of the items included had already been considered in its Opinion on the previous version of the list submitted by the FR SA.

Similarly, for the thirteenth item, the EDPB referred to its previous Opinion, which addressed this kind of processing operation. For the remaining item, it was concluded that the draft list could lead to an inconsistent application of Art. 35 GDPR, so the EDPB recommended changes. Specifically, regarding the management of commercial activities, the FR SA was advised to restrict the scope of this item by covering only business-to-customers relations, and by excluding processing sensitive data or data of a highly personal nature from this item.

Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Art. 28(8) GDPR) Adopted: 19 May 2020

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

Therefore, the EDPB reviews draft SCCs submitted by SAs to contribute to the consistent application of the GDPR throughout the EU.

In February 2020, the Slovenian SA (SI SA) submitted its draft SCCs to the EDPB, requesting an Opinion under Art. 64(1)(d) GDPR. The EDPB made a number of recommendations on how to amend the draft SCCs. The EDPB also recalled that the possibility to use SCCs adopted by an SA does not prevent the parties from adding other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the adopted SCCs or prejudice the fundamental rights or freedoms of the data subjects.

The SI SA amended its draft in accordance with Art. 64(7) GDPR, taking utmost account of the Opinion of the EDPB.

5.3. BINDING DECISIONS

Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR

The EDPB adopted its first dispute resolution decision on the basis of Art. 65 GDPR. The binding decision addressed the dispute that arose after the Irish SA, acting as Lead Supervisory Authority (LSA), issued a draft decision regarding Twitter International Company (TIC) and the subsequent relevant and reasoned objections (RROs) expressed by a number of Concerned Supervisory Authorities (CSAs).

The LSA issued the draft decision based on its own investigation into TIC, after the company notified the LSA of a personal data breach on 8 January 2019.

In May 2020, the LSA shared its draft decision with the CSAs in accordance with Art. 60(3) GDPR. The CSAs then had four weeks to submit any RROs. Among others, the CSAs issued RROs on the infringements of the GDPR identified by the LSA, the role of TIC as the (sole) data controller and the calculation of the proposed fine. As the LSA rejected the objections and/or considered they were not "relevant and reasoned", it referred the matter to the EDPB per Art. 60(4) GDPR, thereby initiating the dispute resolution procedure for the first time. The EDPB officially launched this procedure on 8 September 2020.

The EDPB's decision assessed whether each of the objections raised met the requirements set by Art. 4(24) GDPR. As a result, the main focus of the EDPB's decision was the compliance of the draft decision of the Irish SA with Art. 83 GDPR. Several SAs raised RROs that the proposed fine was insufficiently dissuasive.

With a view to the consistent application of the GDPR, the EDPB decided that the LSA was required to reassess the elements it relied upon to calculate the amount of the fine.

The LSA amended its draft decision by increasing the level of the fine to ensure it fulfilled its purpose as a corrective measure and met the requirements of effectiveness, dissuasiveness and proportionality established by Art. 83(1) GDPR, and taking into account the criteria of Art. 83(2) GDPR.

For further information see: Art. 65 GDPR Frequently Asked Questions

Adopted: 9 November 2020

5.4. CONSISTENCY PROCEDURES

The EDPB may produce documents to enable the consistent application of the GDPR across the EEA, as outlined here.

5.4.1. EDPB document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal

Arts. 42 and 43 GDPR introduce certification as a new accountability tool for data controllers and processors. Certification under Arts. 42 and 43 GDPR can be issued for processing operations by controllers and processors.

Certification under the GDPR shall be issued by accredited certification bodies or by the competent SAs, on the basis of criteria approved by that competent SA or by the EDPB. In this regard, Art. 43(5) GDPR refers to the approval of certification criteria with an EU-wide reach, namely, the European Data Protection Seal.

The EDPB document develops the procedure for the approval of a European Data Protection Seal, focusing on harmonisation and consistency. The approval procedure consists of two phases: an informal cooperation phase and the formal approval phase.

The informal cooperation phase involves all SAs and includes a review of the technical issues linked to the certification criteria, and a national legislation compatibility check. If substantial issues are identified, they can be brought to the relevant EDPB expert subgroup for discussion.

The procedure also foresees the possibility for the scheme owner to ask for clarifications and respond to comments made during the informal phase.

The formal approval phase is based on the procedure for requesting an Art. 64(2) GDPR Opinion. Therefore, the SA submitting the criteria for an Opinion of the EDPB has to provide written reasoning for the request. In this context, the document notes that the SA has to ask for an Opinion under Art. 64(2) GDPR regarding a matter producing effects in more than one Member State. The EDPB Secretariat will then be in charge of drafting the Opinions and, upon decision of the Chair, together with a rapporteur and expert subgroup members.

The EDPB's approval process is completed by the adoption of an Opinion approving or rejecting the EU Data Protection Seal request for the submitted criteria. The EDPB's Opinion is applicable in all Member States.

Adopted: 28 January 2020

5.4.2. EDPB document on the procedure for the development of informal "Codes of Conduct sessions"

The EDPB document develops the procedure for the approval of transnational codes of conduct, focusing on harmonisation and consistency. The approval procedure consists of two phases: an informal cooperation phase and the formal approval phase. The procedures build on Guidelines 01/2019 on Codes of Conduct and, in particular, its Section 8.

The informal cooperation phase involves all SAs and the "Code sessions" are presented as a forum for informal discussions on transnational Codes of Conduct that have not yet been formally submitted to the EDPB, with the aim of finding a consensus on the standards and expectations for Codes of Conduct and making these clear to the code owners. If there is a need for agreements regarding substantial elements of the Codes of Conduct, they can be brought to the relevant EDPB expert subgroup for discussion.

The document further clarifies the nature and format of the Code sessions and elaborates on the role of SAs, and their interaction with both the Competent SAs and the Code owners, as well as on the role of the EDPB Secretariat and the different phases of the approval process.

The formal approval phase is based on the procedure for requesting an Art. 64(1) GDPR Opinion. The EDPB Secretariat, together with two co-rapporteurs, is in charge of drafting the Opinions.

Adopted: 10 November 2020

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

One of the roles of the EDPB is to maintain a publicly accessible electronic register of decisions taken by SAs and courts on issues handled in the consistency mechanism per Art. 70(1)(y) GDPR. This section outlines key decisions taken by various SAs, particularly in response to EDPB Opinions on the topic of their actions.

See Section 5.2.

5.5.1. Approval of Binding Corporate Rules of Fujikura Automotive Europe Group (FAE Group)

As the BCR Lead Supervisory Authority (LSA) in this case, the Spanish SA communicated a draft decision on the Controller BCRs of Fujikura Automotive Europe Group (FAE Group) to the EDPB in accordance with Art. 64(1)(f) GDPR.

The EDPB provided its Opinion 6/2020 (January 2020) on the SA's draft decision. The SA took utmost account of that Opinion and adopted its final decision approving the Controller BCRs of FAE Group in accordance with Art. 47(1) GDPR, finding that the BCRs provide appropriate safeguards for the transfer of personal data to members of the FAE Group established in third countries.

Adopted: 11 March 2020

5.5.2. Decision of the Irish Supervisory Authority approving the Controller Binding Corporate Rules of RGA International Reinsurance Company DAC (RGAI)

As the BCR LSA in this case, the Irish SA communicated a draft decision on the Controller BCRs of RGA International Reinsurance Company DAC (RGAI) to the EDPB in accordance with Art. 64(1)(f) GDPR.

The EDPB provided its Opinion 08/2020 (April 2020) on the SA's draft decision. The SA took utmost account of that Opinion and adopted its final decision approving the Controller BCRs of RGAI in accordance with Art. 47(1) GDPR, finding that the BCRs provide appropriate safeguards for the transfer of personal data to members of the RGAI Group established in third countries.

Adopted: 1 May 2020

5.5.3. Decision of the Irish Supervisory Authority approving the Processor Binding Corporate Rules of RGA International Reinsurance Company DAC (RGAI)

As the BCR LSA in this case, the Irish SA communicated a draft decision on the Processor BCRs of RGA International Reinsurance Group DAC (RGAI) to the EDPB in accordance with Art. 64(1)(f) GDPR.

The EDPB provided its Opinion 09/2020 (April 2020) on the SA's draft decision. The SA took utmost account of that Opinion and adopted its final decision approving the Processor BCRs of RGAI in accordance with Art. 47(1) GDPR, finding that they provide appropriate safeguards for the transfer of personal data to members of the RGAI Group established in third countries.

In its review of the Processor BCRs, the SA concluded that they comply with the requirements set out by Arts. 47(1) and 47(2) GDPR and contain clear responsibilities with regards to personal data processing.

Adopted: 1 May 2020

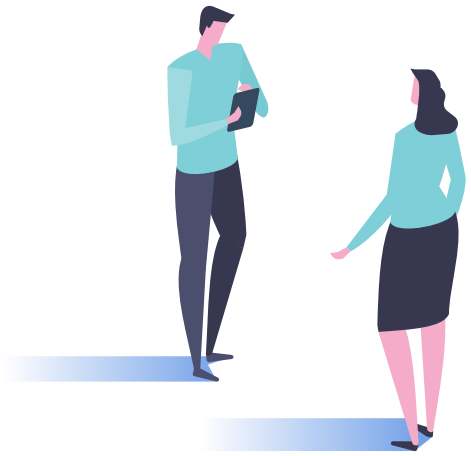
5.5.4. Decision of the Slovakian Supervisory Authority authorising the Administrative Arrangement for the transfer of personal data between EEA Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities

Following the EDPB's Opinion 04/2019, the Slovakian SA authorised the Administrative Arrangement for the transfer of personal data between EEA Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities.

In its decision, the SA noted that the provisions contained in the Administrative Arrangement provide appropriate safeguards for the transfer of personal data between EEA Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities, in accordance with Art. 46(3)(b) GDPR.

The SA will monitor the practical application of the Administrative Arrangement, particularly in relation to data subject rights, onward transfers, redress and oversight mechanisms.

Adopted: 4 May 2020



5.5.5. Irish Supervisory Authority's additional accreditation requirements for certification bodies

The Irish SA adopted the additional accreditation requirements for certification bodies with respect to ISO/IEC 17065/2012 (ISO 17065) and per Arts. 43(1) and 43(3) GDPR. The document contains the requirements necessary to assess the competence, consistent operation and impartiality of certification bodies that intend to issue certifications pursuant to Arts. 42 and 43 GDPR.

As underlined in the requirements, certification under the GDPR is only applicable to processing operations of controllers and processors. In order to issue GDPR certifications, certification bodies must be accredited in accordance with the requirements adopted by the competent SA.

The approval of the additional accreditation requirements by the Irish SA will allow certification bodies that want to issue GDPR certification to apply for accreditation.

Adopted: 1 June 2020

5.5.6. Decision of the Swedish Supervisory Authority approving the Binding Corporate Rules of Tetra Pak Group

As the BCR LSA in this case, the Swedish SA adopted a decision to approve the Controller BCRs of Tetra Pak Group following the EDPB's Opinion 25/2020 (July 2020) on its draft decision.

The SA took utmost account of that Opinion and adopted its final decision approving the Controller BCRs of Tetra Pak Group in accordance with Art. 47(1) GDPR, finding that they provide appropriate safeguards for the transfer of personal data to members of Tetra Pak Group established in third countries.

Adopted: 17 August 2020

5.5.7. Decision of the Norwegian Supervisory Authority approving the Binding Corporate Rules of Jotun Group

As the BCR LSA in this case, the Norwegian SA adopted a decision to approve the Controller BCRs of Jotun to the EDPB following the EDPB's Opinion 24/2020 (July 2020) on its draft decision.

The SA took utmost account of that Opinion and adopted its final decision approving the Controller BCRs of Jotun in accordance with Art. 47(1) GDPR, finding that they provide appropriate safeguards for the transfer of personal data to members of the Jotun Group established in third countries.

Adopted: 18 August 2020

5.5.8. German Supervisory Authorities' requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR

The German SAs amended their requirements for accreditation of a certification body based on Art. 43(3) GDPR in connection with Art. 57(1)(p) GDPR.

The revised requirements are a response to the EDPB's Opinion 15/2020 on the German SAs' draft decision.

The document contains the requirements necessary to assess the competence, consistent operation and impartiality of certification bodies that intend to issue certifications pursuant to Arts. 42 and 43 GDPR. The bodies that want to issue GDPR certification may then apply for accreditation.

As the requirements state, certification under the GDPR is only applicable to processing operations of controllers and processors. Certification bodies must be accredited in accordance with the requirements adopted by the competent SA in order to issue GDPR certifications.

Adopted: 8 October 2020

5.5.9. German Supervisory Authorities' accreditation requirements for a GDPR code of conduct monitoring body pursuant to Art. 41(3) GDPR

The German SAs amended the requirements applicable in Germany for the accreditation of a GDPR code of conduct monitoring body in response to EDPB Opinion 10/2020 on their draft decision. The SAs outlined the administrative and substantive requirements to be fulfilled by the code of conduct monitoring body to receive accreditation.

Approval of the accreditation requirements by the German SAs will allow monitoring bodies to apply for the necessary accreditation in relation to specific GDPR codes of conduct.

Adopted: 8 October 2020

5.5.10. Irish Supervisory Authority's accreditation requirements for a GDPR code of conduct monitoring body pursuant to Art. 41(3) GDPR

The Irish SA adopted the accreditation requirements of a code of conduct monitoring body following the EDPB's Opinion 11/2020 on its draft. In its decision, the SA outlined the administrative and substantive requirements to be fulfilled by the monitoring body to receive accreditation. The requirements include explanatory notes and examples in order to further elaborate on specific requirements or list some elements that may be provided to demonstrate compliance with the requirements.

As established in the GDPR, and underlined in the requirements, the monitoring of compliance with a code of conduct is carried out by accredited monitoring bodies. As such, monitoring bodies are accredited to monitor a specific code of conduct and, therefore, the compliance with the requirements for accreditation has to be demonstrated in relation to a specific code of conduct.

The approval of the accreditation requirements by the Irish SA will allow monitoring bodies to apply for the necessary accreditation in relation to specific codes of conduct.

Adopted: 9 October 2020

5.5.11. Danish Supervisory Authority's accreditation requirements for a GDPR code of conduct monitoring body pursuant to Art. 41(3) GDPR

The Danish SA adopted the requirements applicable in Denmark for the accreditation of code of conduct monitoring bodies following EDPB Opinion 19/2020 on its draft decision.

In its decision, the SA outlined the administrative and substantive requirements to be fulfilled by the monitoring body to receive accreditation.

Monitoring bodies are accredited to monitor a specific code of conduct and, therefore, the compliance with the requirements for accreditation has to be demonstrated in relation to a specific code of conduct.

The approval of the accreditation requirements by the Danish SA will allow monitoring bodies to apply for the necessary accreditation in relation to specific codes of conduct.

Adopted: 12 November 2020

5.5.12. Decision under S.111 of the Irish Data Protection Act 2018 and for the purposes of Art. 60 GDPR in the matter of Twitter International Company

The Irish SA submitted the case of Twitter International Company (TIC) to the consistency mechanism referred to in Art. 63 GDPR as a result of objections raised by other SAs in respect to the Irish SA's draft decision in the case at hand.

The Irish SA began an inquiry on 22 January 2019 to examine whether TIC complied with its obligations to notify the SA of a personal data breach per Art. 33(1) GDPR, and whether TIC adequately documented the breach as per Art. 33(5) GDPR. The final decision was issued on 9 December 2020, in line with Art. 65(6) GDPR, which requires the addressee of an EDPB decision taken on the basis of Art. 65 GDPR to adopt its final decision within one month of the notification of the EDPB decision.

- The Irish SA found that TIC did not comply with its obligations in Arts. 33(1) and 33(5) GDPR and elaborated upon the reasons for this conclusion. In assessing the administrative fine to be imposed as a result, the SA referred to EDPB Decision 01/2020, which requested that the SA reassess the elements upon which the fine is to be determined, and considers the criteria outlined by Art. 83(2) GDPR.

In the matter of TIC's compliance with the requirements found in Arts. 33(1) and 33(5) GDPR, the Irish SA decided to impose an administrative fine of USD 500,000 (EUR 450,000).

Adopted: 9 December 2020

5.6. LEGISLATIVE CONSULTATION

5.6.1. EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic

See Section 3.2.2 for a full summary.

In its draft Guidance on apps supporting the fight against the COVID-19 pandemic, the European Commission proposed the development of a pan-European and coordinated approach in the use of such tools. The EDPB welcomes this initiative and addresses specifically the use of apps for contact-tracing and warning individuals.

5.6.2. Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB

The EDPB adopted its Statement with regards to the role of SAs and the EDPB in the context of the ePrivacy Regulation currently being negotiated. The EDPB highlights the importance of avoiding the fragmentation of supervision, procedural complexity and diverging interpretations through the enforcement of the future ePrivacy Regulation.

In this context, the EDPB underlines that many of the provisions of the future ePrivacy Regulation relate to the processing of personal data and are intertwined with provisions of the GDPR. Thereby the oversight of the ePrivacy Regulation should be entrusted to the same national authorities, which are responsible for enforcement of the GDPR. Further, the EDPB notes that the existing cooperation and consistency mechanism for the supervision and enforcement of the GDPR should also be adopted for the supervision of the ePrivacy Regulation in the context of personal data processing and would lead to more harmonisation and consistency. The same framework would also benefit data controllers through a single point of contact and guarantee a level playing field on the EU Digital Single Market.

Adopted: 19 November 2020

5.7. OTHER DOCUMENTS

5.7.1. Contribution of the EDPB to the evaluation of the GDPR

See Section 3.1 for a full summary.

The EDPB and national SAs contributed to the European Commission's evaluation and review of the GDPR, as required by Art. 97 GDPR. The EDPB considers that the GDPR has strengthened data protection as a fundamental right and harmonised the interpretation of data protection principles, and believes it is premature to revise it at this point in time.

5.7.2. Statement on privacy implications of mergers

The EDPB adopted a statement on privacy implications of mergers having noted the intention of Google LLC to acquire Fitbit, Inc. The EDPB expressed concerns regarding the potentially high level of risk to the fundamental rights to privacy and personal data entailed by the possible further combination and accumulation of sensitive personal data by a major tech company. The EDPB reminded the parties of their obligations under the GDPR and of the need to conduct in a transparent way a full assessment of the data protection requirements and privacy implications of the merger. The EDPB expressed its readiness to contribute further advice on the proposed merger to the European Commission if so requested.

Adopted: 19 February 2020

5.7.3. Statement on the processing of personal data in the context of the COVID-19 outbreak

See Section 3.2.1 for a full summary.

The EDPB emphasises that respecting data protection rules does not hinder the response to the COVID-19 pandemic. Even in exceptional times, data controllers and processors must ensure the protection of personal data.

Adopted: 19 March 2020

5.7.4. Statement on restrictions on data subject rights in connection to the state of emergency in Member States

See Section 3.2.5 for a full summary.

The EDPB emphasises that when EEA Member States enter a state of emergency, such as that brought on by the COVID-19 outbreak, the GDPR remains applicable and allows for efficient emergency response while protecting fundamental rights and freedoms.

Adopted: 2 June 2020

5.7.5. Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak

See Section 3.2.6 for a full summary.

The EDPB urges EEA Member States to adopt a standardised approach to the processing of personal data in the context of reopening borders during the COVID-19 pandemic and emphasises that data processing must be necessary and proportionate.

Adopted: 16 June 2020

5.7.6. Statement on the data protection impact of the interoperability of contact tracing apps

See Section 3.2.7 for a full summary.

The EDPB maintains that, without a common EEA approach in response to the COVID-19 pandemic, an interoperable framework should be put in place regarding contact tracing apps and then outlines seven key focus areas.

Adopted: 16 June 2020

5.7.7. Statement on the Court of Justice of the European Union Judgment in Case C-311/18 – Data Protection Commissioner v Facebook Ireland and Maximillian Schrems

See Section 3.3.1 for a full summary.

The EDPB believes that the CJEU's judgment in Case C-311/18 (*Schrems II*) highlights the importance of the fundamental right to privacy in the context of the transfer of personal data to third countries, and the risk for data subjects caused by possible indiscriminate access by a third country's public authorities to the personal data transferred. Standard Contractual Clauses that enable data transfers must maintain a level of protection in the third country that is essentially equivalent to that in the EEA.

Adopted: 17 July 2020

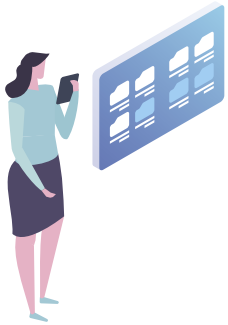
5.7.8. Information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA

The EDPB issued an information note with regards to arrangements for enterprises that have BCRs where the UK SA is the competent SA. In light of Brexit, such BCR holders need to make all organisational arrangements to establish a new BCR Lead SA in the EEA.

The EDPB notes that any current BCR applications before the UK SA are also encouraged to put in place organisational arrangements on the basis of which a new BCR Lead SA in the EEA can be established. This should be completed before the end of the Brexit transition period.

With the aim of providing clarification to BCR holders, the EDPB has a practical checklist of elements that must be amended to ensure their BCRs remain a valid transfer mechanism for transfers of data outside the EEA after the transition period. The same checklist informs applicants with BCRs undergoing review by the UK SA as to which changes need to become effective (at the latest) at the end of the transition period.

Adopted: 22 July 2020



5.7.9. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

See Section 3.3.1 for a full summary.

Following the CJEU's judgment in Case C-311/18 (*Schrems II*), the EDPB provided clarifications on the judgment in a document addressing 12 Frequently Asked Questions (FAQs) about personal data transfers from the EEA to the U.S. and other third countries.

Adopted: 23 July 2020

5.7.10. EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679

In this Document, the EDPB introduces the Coordinated Enforcement Framework (CEF), which builds upon and supports mechanisms for cooperation as outlined in the GDPR.

In this context, the CEF provides a structure for annual coordinated actions by EDPB SAs. The objective of the CEF is to facilitate joint actions, such as joint awareness-raising activities, information gathering and joint investigations. Coordinated actions thus contribute to GDPR compliance, the protection of the rights and freedoms of citizens, and to reducing the risks of new technologies to the right of personal data protection.

In this Document, the EDPB provides an illustrative overview of the structure of the CEF and outlines its lifecycle, stipulates its legal basis and the division of competences between the EDPB and the SAs, as well as indicating the relationship between the CEF and the cooperation and consistency mechanism under the GDPR.

Adopted: 20 October 2020

5.7.11. Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorism financing

The EDPB adopted its Statement following the launch of the public consultation in May 2020 on the European Commission's Action Plan for a comprehensive Union policy for the prevention of money laundering and terrorist financing for a comprehensive Union policy for the prevention of money laundering and terrorist financing. In its Statement, the EDPB reaffirms the existing interplay between the protection of privacy, personal data and anti-money laundering measures, and stresses the need to address this relationship in the updated legislation.

Specifically, the relevance and accuracy of the data collected plays a paramount role, as well as the need to specify a clear legal basis, and define the limits and purposes of personal data processing. The EDPB notes that this is especially pertinent in the context of international data transfers and information sharing, as has also been noted by the EDPS in his Opinion on the same Action Plan.

The EDPB highlights the importance of the compatibility of the anti-money laundering measures with the rights to privacy and data protection, as enshrined in the EU Charter of Fundamental Rights, and the principles of necessity and proportionality.

Adopted: 15 December 2020

5.7.12. EDPB Document on Terms of Reference of the EDPB Support Pool of Experts

Within its mission of ensuring a high and consistent level of protection of personal data throughout the EEA Member States, and as part of its investigatory and enforcement activities, the EDPB adopted the Terms of Reference of its Support Pool of Experts (SPE), which aims to provide material support to EDPB Members and to enhance cooperation and solidarity between all EDPB Members. The SPE comprises both EDPB experts and external experts, and is deployed to assist the carrying out of support investigations and enforcement activities of significant common interest.

The EDPB Document outlines the different types of support activities that the SPE may provide, including analytical support, the preparation of investigative reports and assisting in the performance of findings of a forensic nature. The EDPB notes the legal bases for the creation of the SPE, which are outlined in the GDPR, and elaborates on the key principles of SPE involvement, including the principles of voluntariness, confidentiality and coordination. In its Document, the EDPB also outlines the composition of the SPE, the role of the EDPB and external experts involved therein, as well as the process of reporting and evaluation.

Adopted: 15 December 2020

5.7.13. Pre-GDPR Binding Corporate Rules overview list

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

Adopted: 21 December 2020 (updated on 26 January 2021)

5.7.14. Information note on data transfers under the GDPR to the United Kingdom after the transition period

The first version of the note, adopted on 15 December 2020, described the situation in which transfers of personal data to the UK constitute transfers to a third country. However, the document was updated taking into consideration that on 24 December 2020, an agreement was reached between the EU and the UK. The agreement provides that for a maximum period of six months from its entry into force – i.e., until 30 June 2021 at the latest - and upon the condition that the UK's current data protection regime stays in place, all flows of personal data between stakeholders subject to the GDPR and UK organisations will not be considered as such international transfers.

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

The EDPB recalls the specific information note it has previously issued on the topic, as well as the specific guidance on possible supplementary measures in its Recommendations 01/2020.

Adopted: 15 December 2020 (updated on 13 January 2021)

5.7.15. Statement on the end of the Brexit transition period

The first version of the Statement, adopted on 15 December 2020, was updated taking into consideration that on 24 December 2020, an agreement on future relations was reached between the EU and the UK. The EDPB reminds all stakeholders that the agreement provides that, for a specified period and upon the condition that the UK's current data protection regime stays in place, all transfers of personal data between stakeholders subject to the GDPR and UK entities will not be considered as transfers to a third country subject to the provisions of Chapter V GDPR . This interim provision applies for a maximum period of six months (i.e., until 30 June 2021 at the latest).

The EDPB specifies that, as of 1 January 2021, the One-Stop-Shop (OSS) mechanism is no longer applicable to the UK, so the UK Information Commissioner's Office is no longer part of it.

The EDPB wishes to emphasise that the decision to benefit from the unified dialogue enabled by the OSS mechanism in cross-border processing cases is up to the individual controllers and processors, who to that end may decide whether to set up a new main establishment in the EEA under the terms of Art. 4(16) GDPR.

The EDPB recalls that controllers and processors not established in the EEA, but whose processing activities are subject to the application of the GDPR under Art. 3(2) GDPR, are required to designate a representative in the Union in accordance with Art. 27 GDPR.

Adopted: 15 December 2020 (updated on 13 January 2021)

5.8. PLENARY MEETINGS AND EXPERT SUBGROUPS

Between 1 January and 31 December 2020, the EDPB held 27 plenary meetings. The agendas and minutes of the plenary sessions are published on the EDPB website. During these meetings, the EDPB adopted Guidelines, Opinions and other documents such as statements or information notes to advise the European Commission, national SAs and other stakeholders on GDPR matters, as outlined earlier in this chapter. In addition, there were 145 expert group meetings. In total, 268 meetings were held, including plenary meetings, expert subgroup meetings and drafting team meetings.

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

5.9. STAKEHOLDER CONSULTATION AND TRANSPARENCY

5.9.1. Stakeholder events on future guidance

The EDPB organises stakeholder events to gather input and views on specific issues in the interest of developing future guidance. In 2020, the EDPB organised one such event on legitimate interest. This event was held entirely online due to the COVID-19 pandemic. Participants gave examples of how they had been using legitimate interest as a legal basis for data processing, and highlighted areas that needed clarifying or explaining. The EDPB will use this stakeholder input in the context of drafting future guidance on legitimate interest.

5.9.2. Public consultations on draft guidance

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

To further enhance transparency, the EDPB publishes on its website stakeholders' contributions to public consultations. In 2020, the EDPB launched several such consultations:

- In February, the EDPB opened public consultations on both Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications and Guidelines 02/2020 on Arts. 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies. It received 62 contributions to the Guidelines 01/2020 on connected vehicles, including input from U.S.-based business organisations. Guidelines 02/2020 received contributions from 12 entities, mainly comprising public authorities.
- In July, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR were opened for public consultation. The EDPB received 39 contributions.
- The EDPB published Guidelines 07/2020 on the concepts of controller and processor in the GDPR and Guidelines 08/2020 on the targeting of social media users for consultation in September. 109 entities gave input on Guidelines 07/2020 on controllers and processors, and 33 gave input on Guidelines 08/2020 on targeting social media users.
- In October, Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 were opened for public consultation and received three contributions.
- In December, the EDPB launched public consultations on Guidelines 10/2020 on restrictions under Art. 23 GDPR, which received 11 contributions.
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data were open for public input in November. 193 entities, comprising mainly business associations, submitted responses.

5.9.3. Stakeholder survey on adopted guidance

For the third year in a row, the EDPB conducted a survey as part of the annual review of the EDPB's activities under Art. 71(2) GDPR. Questions centred on the EDPB's work and output in 2020, with a focus on its Guidelines and Recommendations, all with a view to understanding the extent to which stakeholders find the EDPB's guidance helpful in interpreting the GDPR's provisions, and in order to identify future paths to better support organisations as they approach data protection.

5.9.3.1. Participants

Multiple entities, including individual companies and Non-Governmental Organisations, representing different countries, sectors and business sizes, participated in the survey. Businesses and other private organisations were most represented.

5.9.3.2. Findings

In line with the results of the 2019 survey, most stakeholders participating in the 2020 survey found the Guidelines and Recommendations to be helpful in interpreting the GDPR and/or to provide actionable guidance for their activities. The most positive feedback applied to Guidelines 01/2020, 02/2020,

03/2020, 09/2020, 10/2020 and the Recommendation 02/2020. The second most mentioned comment was that, although the Guidelines contained useful and actionable information, they did not answer all the questions of the respondent. This applied in particular to Guidelines 02/2020 and 08/2020. The EDPB's guidance on the concepts of controller and processor, measures to supplement data transfer tools, and consent were notably popular. However, stakeholders considered the Recommendations 02/2020 as not helpful or clear enough. The results showed that participants had consulted, on average, five Guidelines and Recommendations.

Stakeholders were satisfied with the examples used in the EDPB Guidelines and some expressed a desire for further examples, for example with regard to the targeting of social media users. The addition of an executive summary to more Guidelines was well received and respondents would like to see it as a standard section of guidance documents. More often than not, the EDPB guidance triggered a change in the broader strategy of the respondent organisations.

A majority of respondents had participated in at least one EDPB workshop and most who had done so found the overall experience positive. Participants appreciated the useful and insightful information shared by the EDPB during the workshops, especially as they created room for interaction. Similarly, most respondents had participated in the consultation process for certain Guidelines and found the experience positive. Having the possibility to raise concerns created a welcome form of dialogue. Some respondents expressed a desire for more meetings with the relevant stakeholders to enable more input.

Stakeholders mostly found the relevant Guidelines and Recommendations directly on the EDPB website.

5.9.3.3. Conclusions

The EDPB highly appreciated the stakeholders' participation and useful contribution to the EDPB's work. Feedback on the guidance's operational value and alignment with other EU laws was equally appreciated as it gave actionable insights into stakeholder needs. The EDPB also welcomed stakeholders' value of transparency and interest in participating in the adoption process. In 2021, the EDPB is committed to continuing its cooperation and outreach to inform the development and effectiveness of future guidance.

5.9.4. Transparency and access to documents

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

In 2020, there were 42 public access requests registered for documents held by the EDPB.

5.10. EXTERNAL REPRESENTATION OF THE EDPB

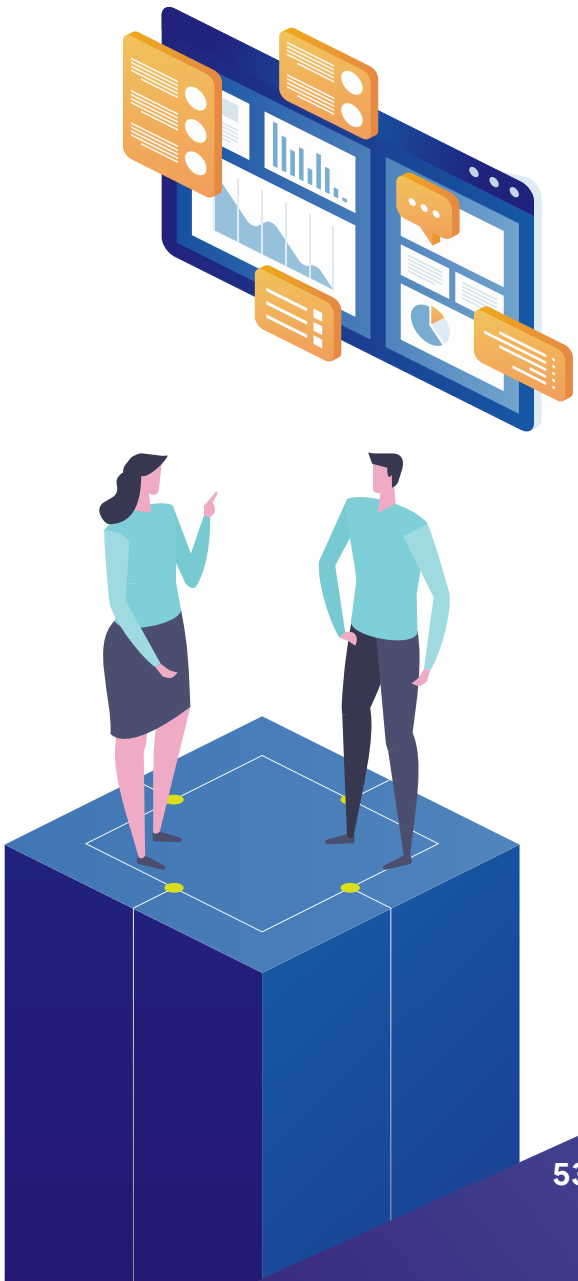
Public awareness and cooperation are vital to upholding data protection rights in the EEA and beyond, which is why the EDPB values stakeholder and citizen engagement. The EDPB Secretariat supports the Chair and Deputy Chairs in engagements with other EU institutions or bodies, and when they represent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

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

In 2020, the Chair of the EDPB, Andrea Jelinek, had over 20 speaking engagements, despite many events being cancelled or postponed due to the COVID-19 pandemic. She gave almost all presentations remotely. The speaking engagements included press briefings, presentations and panel debates for a range of institutes, academic forums and policy agencies. The Chair also met with European Commissioners and representatives from, amongst others, the Committee on Civil Liberties, Justice and Home Affairs Committee of the European Parliament. The Chair engaged with stakeholders beyond the EU. The EDPB Deputy Chair Ventsislav Karadjov took part in four speaking engagements, including speeches and panel presentations.

5.10.2. Participation of EDPB Staff in conferences and speaking engagements

EDPB staff represented the EDPB at a number of events, both in-person and remotely. The events were hosted by, amongst others, universities and trade associations. EU representatives discussed timely issues, such as data protection in the age of the COVID-19 pandemic as well as international data transfers after the *Schrems II* decision.



6

Supervisory Authority activities in 2020

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

These tools are:

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

6.1. CROSS-BORDER COOPERATION

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

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

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

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

Authorities (CSAs). The LSA leads the investigation and drafts the decision, while the CSAs have the opportunity to raise objections.

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

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

In case of conflicting views regarding which SA should act as LSA, the EDPB acts as a dispute resolution body and issues a binding decision. From 1 January 2020 to 31 December 2020, there were 742 instances in which LSAs and CSAs were identified. In 2020, all decisions were made in consensus and no dispute under Article 65.1.b GDPR was brought to the EDPB.

6.1.2. Database regarding cases with a cross-border component

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

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

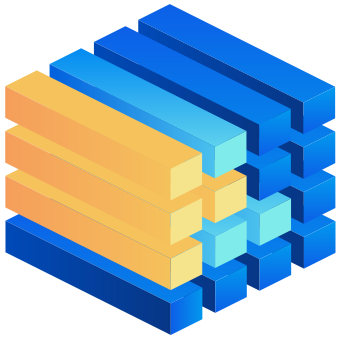
Between 1 January and 31 December 2020, there were 628 cross-border cases out of which 461 originated from a complaint, while 167 had other origins, such as investigations, legal obligations and or media reports.

6.1.3. One-Stop-Shop mechanism

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

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

Once the LSA has completed its investigation, it prepares a draft decision, which it then communicates to the CSAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, the EDPB acts as a dispute resolution body and issues a binding decision. The LSA must adopt its final decision on the basis of the EDPB's decision. If the CSAs do not object to either the initial draft or the revised decision, they are deemed to agree with the draft decision.



Between 1 January 2020 and 31 December 2020, there were 203 draft decisions, from which resulted 93 final decisions.

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

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

The EDPB has published a new public register of the decisions taken by LSAs pursuant to the OSS as a valuable resource to showcase how SAs work together to enforce the GDPR in practice. The relevant LSAs have validated the information in this register in accordance with the conditions provided by their national legislation.

6.1.4. One-Stop-Shop decisions

According to Art. 60(7) GDPR, the Lead Supervisory Authority (LSA) shall inform the EDPB of the final decision taken concerning cross-border cases in the context of the OSS mechanism. According to the GDPR, there is no obligation to make these final decisions public.

Nonetheless, during the 28th Plenary meeting of the EDPB on 19 May 2020, the Members of the EDPB decided to publish a register on the EDPB website relating to these decisions and containing the maximum amount of information possible taking into consideration national limitations.

The register offers an exceptional opportunity to read final decisions taken by, and involving, different SAs in a cross-border context. These decisions often contain interesting guidance on how to comply with the GDPR in practice. The register contains both final decisions and its summaries prepared by the EDPB Secretariat and duly approved by LSAs.

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

As the register was made public in 2020, this Annual Report makes reference to final decisions from the entry into application of the GDPR in 2018 until the end of 2020, during which 168 final decisions were adopted.

6.1.4.1. Selection of cases involving administrative fines

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

Lawfulness of processing / Personal data breach / Security of processing / Administrative fines

LSA: Lithuanian SA

Year of decision: 2019

This case concerned the taking of screenshots by the data controller when a user made an online payment using its service. The user, however, was not notified about the

screenshots being taken. The screenshots recorded personal data of the payer, such as their name and surname, numbers, recent transactions, loans, amounts, mortgages and so on. Moreover, the data controller had provided access to personal data to individuals who were not authorised and did not report the relevant data breach.

Regarding the processing of personal data in screenshots, the LSA considered that this processing by the controller went beyond what was necessary for the performance of the payment service and was also stored for a longer period than necessary. The controller failed to demonstrate the need to collect such an amount of personal data. Moreover, users were not informed of the processing. Therefore, the LSA considered that the processing of personal data was unlawful and that it violated the data minimisation and storage limitation principles.

Regarding the unauthorised access to the personal data, due to a security breach, unauthorised individuals had access to the data concerned, since access could be gained on the controller's website merely by using the identity of the transaction number. The LSA found that the controller failed to implement the appropriate technical or organisational measures to ensure data security. The LSA found that the data controller failed to notify the SA of the relevant data breach as required by Art. 33 GDPR without providing sufficient explanation of that failure to notify.

The LSA decided to impose a fine of EUR 61,500 (2.5% of the controller's total annual worldwide turnover).

Lawfulness of processing

LSA: Maltese SA

Year of decision: 2019

The complainant lodged a complaint with the CSA alleging that the controller kept sending marketing communications to the complainant even though he had previously objected to the processing of his data for marketing purposes. The controller as internal procedure accepted requests from data subjects only when the requests were made using the same email address the users had used to open their accounts.

Through its investigations, the LSA found out that the controller could not find the first email sent by the complainant to object to the processing of his data for marketing purposes even if this email was sent from the email address used by the user to open his account. The data controller admitted that there was a possibility that the email had not been received or had not been dealt with properly.

Following the receipt of further unsolicited marketing communication, the complainant objected several more times. These emails were sent from email addresses different from the one used to open his account. Even if the controller was thus not able to comply with the data subject's request as it could not identify him, the controller decided to block the complainant's account from receiving marketing communications. From the investigation, it appeared that the controller did not have any internal procedures for handling data subject requests. In addition, the controller did not cooperate with the LSA, which had to wait months to receive the requested submissions.

The LSA found that the controller infringed Art. 21 GDPR by not having adequate procedures put in place to deal with the complainant's request to exercise his right to object. The LSA decided that the controller also infringed Art. 31 GDPR by not cooperating with the LSA. Consequently, the LSA imposed an administrative fine of EUR 15,000 on the controller. A EUR 2,000 administrative fine was also imposed on the controller for having breached several provisions of national law relating to unsolicited communications.

Transparency and information / Administrative fines

LSA: Latvian SA

Year of decision: 2019

The complainant alleged that he did not receive information on the identity of the controller before submitting his order on an online retail platform. Moreover, the complainant contended that the privacy policy available on the website was not in conformity with the GDPR.

During its investigation, the LSA found that the controller was a Latvian company performing retail sales through several websites, including the one used by the complainant to order his goods. After establishing the identity of the controller, the LSA found that the privacy policy on the website did not provide information on the identity of the controller, the legal basis of the data processing, its purposes and the way data subjects' consent was collected.

The LSA found that the controller did not comply with its obligations under the GDPR and imposed a fine of EUR 150,000.

Principles relating to processing of personal data / Transparency and information / Administrative fines

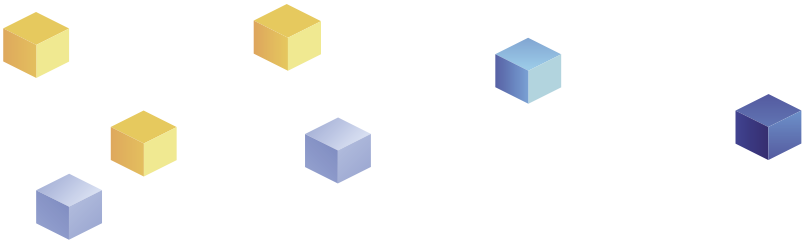
LSA: French SA

Year of decision: 2019

The controller conducted a full and permanent recording of all phone calls from its customer service employees without their ability to object. The controller did not prove that it had limited this processing to what was necessary for the purposes of assessing and training its employees. The controller also recorded the bank details of customers placing orders by telephone when recording its employees' conversations for training purposes and stored such data in clear text in its database for 15 days.

The controller collected copies of Italian health cards and valid identity cards for anti-fraud purposes. The controller also stored a significant amount of personal data of customers who had not connected to their account in over 10 years and of individuals who had never placed an order on the company's website. After the expiry of the storage period for customers' data, the company kept some of their data such as their email address and password in a pseudonymised form for the alleged purpose of enabling customers to reconnect to their accounts. The controller did not inform its customers that their data was transferred to Madagascar. The controller only cited in its privacy policy one legal basis for processing - consent - whereas it conducted several processing operations on different legal bases. The controller did not inform its employees individually of the recording of their telephone calls. The controller accepted user account passwords with eight characters and only one category of characters. It also requested its customers to provide it with a scan of the bank cards used for ordering for anti-fraud purposes. These were subsequently stored by the company in clear-text and containing all of the credit card numbers for six months.

The LSA considered that the controller's recording of all phone calls from its customer service employees, including the bank details of customers placing orders by telephone, and the collection of Italian health cards, which contain more information than the identity card, were not relevant to combat fraud and was excessive. It concluded that it was a breach of the data minimisation principle of Art. 5(1)(c) GDPR. The LSA concluded that the company's storage of a significant amount of personal data of former customers and prospects over long periods that exceeded the purposes for which data were processed violated the storage limitation principle of Art. 5(1)(e) GDPR. The LSA considered that the controller had not informed customers up to a specific date of the transfers of



data to Madagascar nor of the respective legal basis for each processing operation. The LSA also decided that the controller did not adequately inform its employees of the recording of their telephone calls.

All these failings constituted a breach of Art. 13 GDPR (information provided to data subjects). The LSA considered that the type of password authorised by the company did not take sufficient security measures to ensure the security of its customers' bank data, which violated Art. 32 GDPR (security of processing). The LSA provided a detailed indication on how passwords can meet the threshold for "strong passwords". The LSA decided to impose a compliance order on the controller to remedy its breaches of the principles of data minimisation, data storage limitation, requirement to inform data subjects and to ensure data security. It associated the compliance order with a periodic penalty payment of EUR 250 per day of delay on expiry of a period of three months following the notification of this decision.

The LSA also imposed on the controller an administrative fine of EUR 250,000. The LSA further decided to make its decision public on its website, identifying the company by name, for a period of two years.

Lawfulness of processing / Transparency and information / Right to erasure / Administrative fines

LSA: Spanish SA

Year of decision: 2020

The LSA received two separate complaints related to the processing of personal data through the controller's mobile app for Android, from complainants who received prank calls via the controller's application. This app allowed its users to carry out telephone pranks on third parties. The user selected a prank, and a third party (a "victim") was then contacted by phone through a hidden number via the controller's application. The audio of the conversation was recorded and made available to the user. The user was able to share the recording on social media. The third party was not asked for consent for processing of his/her personal data.

The LSA considered that the controller carried out the processing without first informing data subjects, namely, the people receiving the prank call. As such, the data subjects were not aware of the controller's processing of their personal data. The controller claimed that it processed personal data based on the legitimate interest as per Art. 6(1)(f) GDPR. However, the controller did not inform data subjects of its use of the legitimate interests of the controller or of a third party as a legal basis for processing.

The LSA decided that the controller's processing of data was not necessary for the purposes of the protection of its legitimate interests, nor did these interests outweigh the fundamental rights and freedoms of the data subject to the protection of his/her personal data. The LSA concluded that the legitimate interest referred to in Art. 6(1)(f) GDPR could be used as a legal basis for the processing of personal data in this case. Consent also could not serve as a legal basis in this data processing act. The conditions it requires, such as being informed, were not met. The LSA concluded that the processing carried out by the controller could not, under any circumstances, be regarded as lawful and violated Art. 6 GDPR.

For the infringement of Arts. 13 and 14 GDPR and the infringement of Art. 6 GDPR, the LSA imposed two administrative fines, each of EUR 20,000.

The LSA also required the controller to ensure compliance with the rules on personal data protection relating to its processing operations within three months, including the information it provides to its clients and the procedure by which they must give their consent to the collection and processing of their personal data.

Personal data breach / Administrative fines

LSA: United Kingdom SA

Year of decision: 2020

On 22 June 2018, an unidentified attacker gained access to the data controller's IT systems via CAG (a tool that allows users to remotely access a network) and maintained this ability to access without being detected until 5 September 2018. After gaining access to the wider network, the attacker traversed across the network. This culminated in the editing of a JavaScript file on the controller's website. The edits made by the attacker were designed to enable the exfiltration of cardholder data from that website to an external third-party domain, which the attacker controlled. The controller was alerted by a third party about the exfiltration of personal data from the controller's website and then notified the LSA about the attack on 6 September 2018.

The controller estimated that 429,612 data subjects were affected. The affected categories of personal data were username and passwords of contractors; employees and members of an executive club; customer names and addresses; and unencrypted payment card data including card numbers, CVV numbers and expiry dates. The controller took immediate measures to mitigate and minimise any damage suffered by the data subjects by implementing remedial measures, including notifying banks and payment schemes, the data subjects and data protection regulators; cooperating with regulatory and governmental bodies; and offering reimbursement to all customers who had suffered financial losses as a direct result of the theft of their card details. The controller also implemented a number of remedial technical measures to reduce the risk of a similar attack in the future.

The LSA found that the controller failed to process the personal data of its customers in a manner that ensured appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Art. 5(1)(f) and Art. 32 GDPR. The LSA concluded that there are a number of appropriate measures that the controller could have considered to mitigate the risk of an attacker being able to access the controller's network. The LSA considered that each step of the attack could have been prevented, or its impact mitigated, by the controller's implementing one or more of those appropriate measures that were open to the controller. The LSA also considered that, had the controller performed more rigorous testing or internal penetration tests, it would have likely detected and appropriately addressed many of the data security problems identified.

The LSA concluded that the infringements constituted a serious failure to comply with the GDPR. The LSA decided to impose an administrative fine of GBP 20,000,000 on the controller after having taken into account a range of mitigating factors and the impact of the COVID-19 pandemic.

Personal data breach / Administrative fines

LSA: United Kingdom SA

Year of decision: 2020

The personal data breach in this instance related to exposed personal details, such as names, payment card numbers, expiration dates and CVV numbers. 9,400,000 EEA data subjects, of whom 1,500,000 were in the UK, were notified as having been potentially affected by the personal data breach. The personal data breach related to compromised bankcard details and transaction fraud on bank accounts. One bank suggested that around 60,000 individuals' card details had been compromised, while another bank suggested that around

6,000 payment cards had needed to be replaced as result of the controller's transaction fraud. The controller received around 997 complaints from individuals claiming economic loss and/or emotional distress. The controller was not able to provide a detailed analysis of the individuals affected to the SA.

The LSA found that the controller had failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Art. 5(1)(f) and Art. 32 GDPR. In addition, the LSA found that the controller failed to detect and remediate the breach in a timely manner or provide a fully detailed analysis of the individuals affected to the LSA within 72 hours of having detected the personal data breach. Furthermore, the LSA considered mitigation factors, such as the fact that the controller forced password resets across all its domains and created a website where customers could access information about the personal data breach.

In view of the above, the LSA imposed an administrative fine of GBP 1,250,000 on the controller.

Personal data breach / Security of processing / Administrative fines

LSA: United Kingdom SA

Year of decision: 2020

The controller for the data processing activity at stake acquired a company whose IT systems were infiltrated by an attacker before the acquisition. The controller was not aware of the infiltration during the acquisition, nor did it become aware of this afterwards. The controller realised the infiltration once the attacker triggered an alert in relation to, amongst others, a table containing cardholder data. The attacker appeared to have obtained personal data in both an encrypted and unencrypted form. The unencrypted personal data contained data from the guest profile, including reservation and consumption data of customers, while the encrypted information contained 18,500,000 encrypted passport numbers and 9,100,000 encrypted payment cards. Subsequently, the controller informed the data subjects and took steps to mitigate the effects of the attack. Finally, the controller notified the LSA of the personal data breach.

The LSA investigated the case and found that the controller did not ensure appropriate technical and organisational measures to ensure an appropriate level of security as required by Art. 5(1)(f) and Art. 32 GDPR. In particular, the LSA found that the controller did not sufficiently monitor the privileged accounts and the databases. In addition, the LSA found that the controller failed to ensure that the actions taken on its systems were monitored appropriately and that the controller did not apply encryption to all the passport numbers, as it should have.

The LSA, considering the relevant mitigating factors, imposed an administrative fine of GBP 18,400,000 on the controller.

6.1.4.2. Other cases on the interpretation of GDPR provisions

Lawfulness of the processing

LSA: North Rhine-Westphalia SA

Year of decision: 2018

The complainant stated they received postal advertising and tried to exercise their right of access and right to erasure. The complainant contacted their local SA as they deemed that the controller was wrongfully processing their personal data. The data used by the controller was collected from a publicly accessible register.

The LSA underlined that recital 47 and Art. 6(1)(f) GDPR provide for the possibility for data controllers to rely on legitimate interest for the processing of personal data for marketing purposes. As the data were already publicly accessible, the LSA argued that the data subject did not present any prevailing fundamental rights and freedoms, and neither were prevailing rights and freedoms apparent. The LSA decided that the processing of publicly available personal data for direct marketing purposes may constitute lawful processing according to Art. 6(1)(f) GDPR.

Regarding the data subject requests, the original access and erasure requests were filed before 25 May 2018 and Arts. 13 and 14 GDPR were thus not yet applicable. The LSA underlined that these articles require data controllers to inform data subjects of which source the personal data originate. The LSA requested that the controller provide this information for future advertising mail.

The LSA concluded that there was no GDPR infringement.

Request to erasure / Identity authentication

LSA: French SA

Year of decision: 2019

The complainant stated that the right to erasure had been refused by the controller. The controller requested a scan of the complainant's identity document and their signature, although neither of the two were required upon creating the relevant account.

The LSA found that the controller systematically requested that individuals provide a copy of an identity document for exercising their rights, regardless of their country of residence and without providing a basis for reasonable doubts as to the identity of the complainant according to Art. 12(6) GDPR. As such, the LSA found that the controller required disproportionate information for the purpose of verifying the identity of the data subject. The SA stated that it is disproportionate to require a copy of an identity document where the claimant has made their request where they are already authenticated. An identity document may be requested if there is a suspicion of identity theft or account piracy, for instance.

In addition, the LSA underlined that a controller may only store information needed for the exercise of individuals' rights until the end of the applicable legal limitation periods. During this period, the data have to be subject to an "intermediary" archiving on a support base separate from the active base with restricted access to authorised persons.

The LSA issued a reprimand against the controller.

Interpretation of Art. 24 GDPR

LSA: Czech SA

Year of decision: 2019

A complaint was filed with a CSA concerning the processing of personal data of the users of antivirus software provided by the controller, and specifically the protection granted to users of the free version of the software compared to that granted to the paying users.

In its inspection report, the LSA concluded that the inspected party failed to comply with Art. 5(2) and Art. 24(1) GDPR. This was interpreted as the obligation to take into account all relevant circumstances surrounding the processing and to adopt a set of measures to ensure that all personal data processing is carried out exclusively under pre-defined conditions that the controller is able to regularly check and enforce. This stemmed from the conclusion – based on Court of Justice of the EU jurisprudence - that the inspected party, despite its assertions to the contrary, was indeed processing personal data (such as IP addresses) and was acting as a data controller.

The controller filed several objections to the inspection report, arguing, amongst others, that no processing of personal data was involved, that it was not a data controller, and that sufficient information to properly show compliance with Art. 5(2) and Art. 24(1) GDPR was provided. The last objection was partially accommodated by the LSA, which concluded that only an infringement of Art. 24(1) GDPR had been ascertained, whereas no specific breach of Art. 5(2) GDPR followed from the documentation.

The controller was found to have violated Art. 24(1) GDPR.

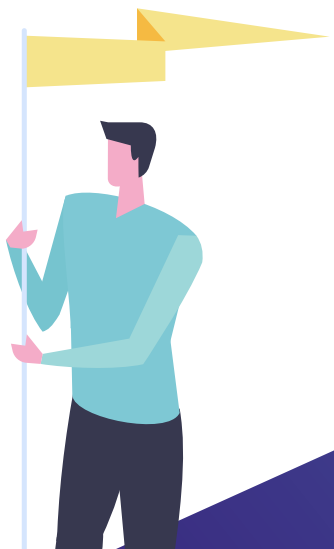
Request for access / Identity authentication

LSA: Brandenburg SA

Year of decision: 2019

The complainant requested access to his personal data processed by the controller. The controller verified the data subject's identity, and subsequently informed the complainant that his account had been suspended due to a discrepancy between the information concerning the age on his account and the information he had provided for the verification of his identity for the request. Since he was 15 years old at the time and thus a minor, he was also asked to send parental consent, a copy of his identity card and a birth certificate to access his personal data. The complainant filed a complaint to the CSA on the understanding that the information he had provided for the verification process was wrongly used to suspend his account instead of being used for the process of giving access to personal information.

The controller underlined that at the time of the request there was no standardised process in place within the company for requests by minors, since the contractual relationship between the controller and the data subjects depends on the fact that the data subjects are adults. Shortly after the controller requested additional documentation for parental consent, this request was set aside and access to personal data was given to the complainant. Finally, further measures were taken by the controller to improve the data access process.



The LSA decided that the request for information was answered in due time and the controller's verification process had been modified in a suitable manner. The LSA therefore found that there was no infringement of the GDPR.

Lawfulness of publication - legitimate interest

LSA: Czech SA

Year of decision: 2019

The data subject filed a complaint with one of the CSAs alleging that the controller published his personal data on its social media page without a legal basis. The controller published information concerning the complainants and other data subjects, referring to debts that the controller was in charge of collecting, on its social media page. The abbreviated first name and the entire surname of the data subjects, as well as the status of debtor and the amount owed by them were specified.

The controller argued it did this on the basis of its legitimate interest. The LSA provided a detailed assessment of the conditions for legitimate interest to be a lawful legal basis. According to the LSA, the controller's legitimate interests must first of all be lawful, i.e., in compliance with legal regulations, and clearly formulated (not speculative). These legitimate interests also include economic interests, i.e., interest in securing the economic side of its business operations. The processing must also be necessary for the purposes of the legitimate interests of the respective controller or third party, i.e., it is not possible to achieve the same result by processing a narrower scope of personal data or infringing the data subjects' rights to a lesser degree. Finally, the interests or rights and freedoms of the data subjects should not take precedence over the alleged legitimate interests. The LSA explained that in this assessment it is also necessary to take into account the nature and importance of the controller's legitimate interests, the impact of the respective processing on the data subjects, including the data subjects' reasonable expectations and any other protective measures applied by the controller.

The LSA decided that the controller had other less intrusive means to fulfil its interests. In addition, the interests and rights of the data subject prevailed over those interests, given the significant risk of adverse impact arising from the publication of negative information about the data subjects' financial situation. Such information could lead to the social exclusion of such persons and their family members, loss of employment and other negative implications. Moreover, data subjects had reasonable expectations of data not being disclosed.

As a result, the LSA considered that the interests of the controller or any third parties were outweighed by the data subject's interests and basic rights and freedoms requiring protection of personal data. The LSA ordered the controller to cease processing of the complainant's personal data and to remove the published personal data within 10 business days of the decision. The LSA also ordered the controller to submit a report to the LSA on the implementation of the order within five business days of its completion.

Data subject rights

LSA: Hessen SA

Year of decision: 2019

The complainant filed a complaint with the CSA contending that the controller did not comply with his access request within the one-month period, as established in Art. 12(3) GDPR.

When contacted by the LSA, the controller explained that the number and complexity of the data-related customer queries at the time of the request justified an extension of the one-month period. Additionally, by mistake, no notice of the extension had been sent to the complainant within the deadline. However, shortly after the deadline, the controller did

send the complainant a notice of the extension. The access request was complied with within the extended timeframe.

The LSA found that there was an infringement of Art. 15 GDPR since the controller did not comply with the complainant's access request in the established timeframe and issued a reprimand to the controller. However, the LSA considered that the controller had cooperated with the LSA during the investigation and notified the complainant of the justified need for an extended timeframe shortly after the due date and answered the request within the extended timeframe. Therefore, the LSA decided not to take any further measures against the controller.

Interpretation of Art. 12(6) GDPR concerning identity authentication

LSA: Danish SA

Year of decision: 2019

The complainant requested to have his personal data deleted from the controller's database. The controller replied that, before processing his erasure request, a proof of identification was necessary to confirm his identity. As the complainant refused to comply with the controller's demand, his data was not deleted.

The LSA found that the controller's procedure under which identification validation was required without exception when processing a data subject's request was not in conformity with Art. 12(6) and Art. 5(1)(c) GDPR. The LSA also found that, under the controller's procedure, data subjects had to provide more information than initially collected in order to have their request processed. Consequently, the controller's procedure for identification validation went beyond what was required and made it burdensome for data subjects to exercise their rights.

The LSA decided that the processing was not done in accordance with Art. 12(6) and Art. 5(1)(c) GDPR. It ordered the controller to decide within two weeks whether the conditions for erasure present in Art. 17 GDPR were met and, if so, to delete the complainant's data.

Adequately informing data subjects and securing their data

LSA: French SA

Year of decision: 2019

The LSA conducted two on-site investigations at the controller's premises to audit the controller's compliance with the GDPR and tested the procedure set up by the controller to create an account.

The controller is a company offering subscriptions to educational magazines for children. On the basis of the investigation, the LSA found several GDPR infringements. First, several breaches of the obligation to inform data subjects, enshrined in Art. 12 and Art. 13 GDPR, were identified. No information relating to data protection nor a link to the controller's Terms and Conditions was given to data subjects upon registration or when placing an order. As a consequence, the information was considered to be not accessible enough. The Terms and Conditions did not include any information on the legal basis for processing, the retention period and the individual rights to restriction of processing, data portability, or to submit a claim to an SA. Although the target audience was French-speaking and the website is fully in French, the "unsubscribe" button in the newsletter and marketing emails was hyperlinked to a text in English, asking for confirmation. An additional hypertext link was included in the final page (titled "Clicking here"). The LSA considered this link misleading for the users, as clicking on it actually resulted in a new subscription.

Second, a breach of the obligation to comply with the request

to erase data was identified, as personal data was not erased systematically when requested by data subjects although there was no legal requirement to keep it and although users had been informed of the erasure of the data. Third, there was a breach of the obligation to ensure the security of data, concerning passwords, locking of workstations and access to data. More specifically, the password requirements and methods for processing the passwords were found to be non-compliant with the obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, since authentication was based on insufficiently complex passwords and obsolete hash algorithms. Additionally, the computer used by one of the database's administrators was configured to never automatically lock or go on sleep mode. With regard to access to data, the absence of specific identification (i.e., the use of the same account by several people) made it impossible to ensure access traceability.

The LSA ordered the controller to comply, within two months of the notification of the decision, with several specific instructions. First, the controller was ordered to provide full information to data subjects about the processing activities in an easily accessible manner. Additionally, the LSA ordered the controller to set up a procedure for unsubscribing that is compliant with Art. 12 and Art. 21 GDPR. Second, the controller was ordered to ensure the effectiveness of all requests to exercise the right of erasure. Third, the authority ordered the controller to take appropriate security measures to protect personal data and prevent access thereto by unauthorised third parties by setting up a new password policy, avoiding the transmission of passwords in clear text, ensuring that workstations go on sleep mode and setting up individual accounts.

Lawfulness of data processing

LSA: French SA

Year of decision: 2020

The complainants encountered difficulties exercising their right to object to direct marketing and rights of access and portability.

The LSA found out during the investigation that an incident arose during the migration of the controller's consent management tool for marketing communications, causing consents not given/withdrawn considered as given/not withdrawn, and the users' communication preferences not to be taken into account in the controller's communication campaigns.

Although the LSA noted that the problem had been solved and that the users' communication preferences had been restored, it stemmed from this incident that, before the migration of its consent management tool, the controller had not implemented the necessary measures as required by Art. 24 GDPR.

The LSA also found that the controller's procedure to process access requests was not fully compliant with Art. 32 GDPR. Indeed, the LSA noted that, in the absence of a client account, the username and password for connection to content containing personal data were sent to data subjects via the same channel. The LSA stated that it was the controller's duty to communicate the username and password for connection via two different communication channels.

As such, the controller was asked to modify this procedure. The LSA determined that the controller had improved the procedures to handle data subject rights requests and trained employees on such procedures.

The LSA issued a reprimand to the controller.

Data subject rights in the context of marketing

LSA: Hungarian SA

Year of decision: 2020

The complainant lodged a complaint against the controller with one of the CSAs after receiving unsolicited marketing messages. The complainant asked to unsubscribe on several occasions without success.

The LSA requested that the complainant make a statement within eight days to disclose his identity to the controller in the course of the procedure, warning that without disclosing his identity, the investigation could not be conducted. The LSA also requested a copy of the erasure request addressed to the controller, as well as copies of any other communication and correspondence with the controller and the controller's response to the erasure request.

The LSA repeated this request a number of months later as there was no response from the complainant. In the absence of a response, the LSA examined the documents made available to it by the CSA. It was not possible to establish from the screenshots enclosed when the complainant unsubscribed from the controller's newsletter or on how many occasions. The documents were not dated, and email addresses were not visible or available. The screenshots of the electronic newsletters of the controller did not reveal the addressee nor the email address that they were sent to.

As the complainant's request remained unverified, no decision establishing an infringement was made. The LSA rejected the complaint without an investigation of merit.

Right to object / Right to erasure

LSA: Austrian SA

Year of decision: 2020

The complainant informed the CSA that he had been receiving advertising emails for months. Attempts to unsubscribe had been unsuccessful and appeared to generate further spam emails. The complainant subsequently contacted the CSA to request assistance with enforcing his objection to the unsolicited spam emails.

The complainant did not contact the controller regarding the assertion of his rights as a data subject concerned. The LSA considered that, following Art. 12 GDPR, the rights under Art. 15 to Art. 22 GDPR require a request by the data subject. Such requests for information or objection were not made to the controller. Therefore, the complaint was dismissed and the CSA to which the complaint was submitted was called to take the final decision in accordance with Art. 60(8) GDPR and to notify the complainant and the controller.

Right of access

LSA: Cypriot SA

Year of decision: 2020

The complainant sent an email to the controller requesting the closure of his account and access to his data on the basis of Art. 15 GDPR. According to the complainant, the controller did not reply to the access request, so he lodged a complaint with the SA.

The LSA found that the email sent by the complainant, wherein he requested access to his data, was never received as it was flagged by the email security service and categorised as spam due to the applied information security IT measures for emails

received from outside the controller. The account manager who also received the email assumed that it had an informative character and was under processing, since the established procedure for an account closure is to be forwarded only to the team responsible for this (Customer Support Team).

Since the controller affirmed that it was working with the IT department to find a solution to avoid similar incidents in the future and that it planned on organising training sessions for staff that interact with the clients, the LSA decided not to take further actions regarding this matter.

6.1.5. Mutual assistance

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

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

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

Between 1 January 2020 and 31 December 2020, SAs initiated 246 formal mutual assistance procedures. They initiated 2,258 informal such procedures.

6.1.6. Joint operations

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

In 2020, SAs carried out one joint operation.1

6.2. NATIONAL CASES

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

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

6.2.1. Some relevant national cases with exercise of corrective powers

SAs play a key role in safeguarding individuals' data protection rights. They can do this through exercising corrective powers. The EDPB website includes a selection of SA supervisory actions. This section of the Annual Report contains a non-exhaustive list of certain enforcement actions in different EEA countries. Several cases highlighted a lack of proper technical and organisational measures for processing personal data securely, which led to data breaches. Many other cases revolved around data processing without a data subject's consent. Some significant incidents involved the unlawful processing of special categories of personal data, such as health data. Numerous cases also involved data subjects who could not

effectively exercise their rights, such as the right of access, the right to erasure and the right to object to a processing act. The entities fined were from both the private and the public sectors.

6.2.1.1. Austria

The Austrian SA carried out multiple investigations and gave several warnings during 2020. For example, the SA carried out investigations into various data controllers that operate customer loyalty programmes. The controllers were seeking the consent of data subjects to process their personal data for the purpose of profiling and to personalise advertising. The request for consent was placed at the end of the registration form of the customer loyalty programme. Among other things, it was ruled that the requested consent was invalid as an average data subject would assume that a signature field placed at the end of a customer loyalty programme registration form is a signature to confirm the registration for the programme and not a signature to provide the consent for the processing of personal data. The controllers appealed this formal decision, meaning the case is still pending before the respective Austrian courts.

The Austrian SA also carried out investigations into the Public Employment Service of Austria (AMS). The AMS used an algorithm to evaluate the employment opportunities of unemployed people. It was ruled that there was no sufficient legal basis for using such programmes and that the personal data processing of unemployed people for this purpose was unlawful. The AMS appealed this formal decision and the Austrian Federal Administrative Court subsequently ruled that, contrary to the opinion of the Austrian SA, a sufficient legal basis exists for this processing. The case is currently pending before the Austrian Administrative High Court.

On 11 November, the Austrian SA issued a warning to the Federal Ministry of Social Affairs, Health, Care and Consumer Protection nothing that the intended processing operations in the context of the electronic COVID-19 vaccination passport were likely to violate the GDPR. The scope of the encroachments on the fundamental right to data protection were not clear from the legislation itself, however, provisions relating to the vaccination passport did not meet certain GDPR requirements, particularly with regard to transparency, the allocation of roles, data subject rights and statistical evaluations.

6.2.1.2. Belgium

The Belgian SA published 31 decisions in 2020. This section lists some key decisions.

On 29 May, the Belgian SA imposed a fine of EUR 1,000 on a controller for not responding to a request from a citizen to object to the processing of his data for marketing purposes and for not collaborating with the SA.

On 8 June, the Litigation Chamber of the Belgian SA issued a fine of EUR 5,000 to a candidate in local elections for using the staff registry of a Municipality to send election propaganda, in the form of a letter, to staff members. The Belgian Municipality in question filed the complaint against the candidate.

On 16 June, the Belgian SA imposed a fine of EUR 1,000 on an association that, on the basis of its legitimate interest according to Art. 6(1)(f) GDPR, sent direct marketing messages to former and current donors for its fundraising efforts. The administrative fine was imposed following a complaint lodged with the Belgian SA by a former donor of the association as the association had not complied with the request for data erasure addressed by the individual to the data controller pursuant to the right to erasure and the right to object to processing. The Litigation Chamber thus decided that the data controller had infringed multiple GDPR provisions.

On 19 June, the Belgian SA issued a fine of EUR 10,000 to a controller for sending a direct marketing message to the wrong person and for not responding adequately to the data subject's

subsequent request for access to his data.

On 14 July, the Belgian SA imposed a EUR 600,000 fine on Google Belgium for not respecting the right to erasure of a Belgian citizen, and for a lack of transparency in its request form to delist.

On 30 July, telecom operator Proximus was fined EUR 20,000 for several data protection infringements regarding personal data processing for the purpose of publishing public telephone directories.

On 8 September, the SA issued a warning and reprimand to a regional public environmental institution for wrongful processing of personal data from the National Register. The Litigation Chamber of the Belgian SA may not impose an administrative fine on a Belgian public institution or any other government body as this was excluded by the Belgian legislator.

On 24 November, the Belgian SA issued a fine of EUR 1,500 for unlawful processing of personal data through a video surveillance system. The Belgian SA also concluded that the positioning of the cameras in the video system constituted an infringement of the data protection by design principle.

6.2.1.3. Bulgaria

The Bulgarian SA experienced an increase in the number of complaints received and the actions taken in 2020. The Bulgarian SA issued a total of 426 decisions as a result of complaints it handled, and imposed administrative sanctions amounting to a total of BGN 518,700 (EUR 265,207). Most violations were made by data controllers processing personal data via established video surveillance systems as well as in the sphere of telecommunication services, media, banks and marketing companies. This section expands upon a selection of interesting cases.

- Several cases concerned political parties or other organisations, which were involved in the procedure set for organising the EU parliamentary and local elections, where they submitted lists with supporters to participate in the elections and did not set clear procedures for verifying the personal identification data entered in the list, thus allowing falsification of signatures and the misuse of the Unified Civil Number of Bulgarian citizens. Since the cases concerned one or two individuals, the lack of procedure did not affect a large number of citizens, however in some of cases the parties in question had already been sanctioned for similar violations;
- A communal services provider was sanctioned for misusing an individual's personal data in case of debt insolvency, which led to the involvement of a private bailiff and a consequent payroll seizure. When imposing the fine, the Bulgarian SA considered the serious adverse effect suffered from the individual as a result of the violation and negligence with which the individual's personal data was handled by the employee and the practice on similar cases with the same type of violations;
- A magistrate, being a public person, issued a complaint about the publishing of a document, submitted by him by electronic media, without blurring his signature. In this case, the Bulgarian SA stated that despite the clear role of the electronic media as a provider of information for public interest purposes, leaving the signature of the public person had no added value and thus should have been blurred by the controller when publishing the provided document. The SA also considered that the violation was not the first one for this electronic media and the person concerned suffered negative consequences. The Bulgarian SA imposed an administrative sanction on the data controller and ordered it to bring its processing operations into compliance with the GDPR by minimising the published data;
- The Bulgarian SA handled a case about the requested erasure of a businessman's arrest photos, published by the media, who was acquitted by the court for corruption;

- Another case pertained to the dissemination of personal data by a state authority in connection with a corruption signal submitted to it;
- The Bulgarian SA also handled a case about a person who served a prison sentence and, once the 10-year statute of limitations expired, requested erasure of their personal data due to the expired public interest.

6.2.1.4. Cyprus

The Cypriot SA fined LGS Handling Ltd, Louis Travel Ltd and Louis Aviation Ltd (Louis Group of Companies) EUR 82,000 for the lack of legal basis of the "Bradford Factor" tool, which was an automated tool used to score the sick leave of employees. The Cypriot SA launched an investigation after the employees' trade union lodged a complaint. Importantly, it had not been established that the legitimate interest of the controller overrode the interests, rights and freedoms of its employees.

On 17 June, the Cypriot SA imposed a fine of EUR 15,000 on the Bank of Cyprus Public Company Ltd for the loss of a client's data, which specifically infringed Arts. 5(1)(f), 5(2), 15, 32 and 33 GDPR.

6.2.1.5. Czech Republic

The Czech SA fined a used car dealer CZK 6,000,000 for repeatedly sending unsolicited commercial communications. This was the highest fine the office imposed for this kind of breach. The company continually distributed electronic commercial communications to recipients who had not granted consent.

6.2.1.6. Denmark

Unlike in other EEA jurisdictions where the SAs have the authority to issue administrative fines themselves, in Denmark, the Danish SA first investigates a data protection legal violation and then reports it to the police. The police then investigate whether there are grounds for raising a charge and finally a court decides on a possible fine.

In June, the Danish SA proposed that the Municipality of Lejre be fined DKK 50,000 for failing to comply with its obligation as a data controller to implement appropriate security measures. Its department called the Centre for Children and Young People had a fixed practice where meeting minutes containing personal information of a sensitive and protected nature, including information about citizens under the age of 18, had been uploaded on the Municipality's employee portal where a large part of the employees could access this. In July, the Danish SA reported ARP-Hansen Hotel Group to the police and proposed a fine of DKK 1,100,000 for the failure to delete approximately 500,000 customer profiles, thus violating the storage limitation requirement in Art. 5(1)(e) GDPR.

In December, the Danish SA reported the Municipality of Guldborgsund to the police and proposed a fine of DKK 50,000. The Municipality had mistakenly sent a decision via Digital Post containing information about the complainant's child's place of residence to the complainant's child's father, even though the father had been deprived of custody, thus amounting to a security breach that had major consequences for the complainant and the child. The Municipality had failed to notify the complainant and the SA of the security breach.

6.2.1.7. Estonia

On 30 November, the Estonian SA granted a warning, with a one-day compliance deadline and a penalty of EUR 100,000, to three pharmacy chains that had allowed people to view the current prescriptions of other people in the e-pharmacy environment, without their consent, on the basis of access to their personal identification code.

6.2.1.8. Finland

This section sets out five pertinent instances in which the Finnish SA imposed fines for violations of data protection law.

On 18 May, the sanctions board imposed three administrative fines. First, for deficiencies in information provided in connection with change-of-address notifications, the board fined Posti Oy EUR 100,000. Second, because it had neglected to conduct a Data Protection Impact Assessment for the processing of employee location data, the sanctions board imposed an administrative fine of EUR 16,000 on Kymen Vesi Oy. Third, the board imposed a fine of EUR 12,500 on a company because it had collected job applicants' personal data unnecessarily.

On 26 May, the Finnish SA imposed an administrative fine on Taksi Helsinki Oy for violations of data protection legislation. The company had not assessed the risks and effects of personal data processing before adopting a camera surveillance system that recorded audio and video in its taxis. The Finnish SA noted deficiencies in the information provided to customers and the documentation of personal data processing. The sanctions board imposed an administrative fine of EUR 72,000 on Taksi Helsinki.

In July, the sanctions board of the Finnish SA imposed an administrative fine on Acc Consulting Varsinais-Suomi for sending direct electronic marketing messages without prior consent as well as neglecting the rights of data subjects. The company did not respond to or implement the requests concerning the rights of data subjects, and it was not able to prove that it had processed personal data legally. The sanctions board therefore imposed a financial sanction of EUR 7,000 in addition to several corrective measures for the company to complete.

6.2.1.9. France

France had several important cases with comparably large fines in 2020. Such cases pertained to the following entities: SPARTOO, Carrefour France and Carrefour Banque, Google LLC and Google Ireland Ltd, and Amazon Europe Core.

In applying the one-stop-shop mechanism, the French SA acted as the LSA in a cross-border enforcement case involving thirteen EEA countries. The French SA found that SPARTOO, which specialises in the online shoe sales sector, had failed to comply with the following obligations: to adhere to the data minimisation principle; to limit the data retention period; to inform data subjects adequately about how their personal data would be processed; and to ensure data security. In August, the French SA imposed a fine of EUR 250,000 and issued an injunction to the company to comply with the GDPR.

In November, the French SA issued fines of EUR 2,250,000 to Carrefour France and EUR 800,000 to Carrefour Banque for violations of data protection law. Most of the violations pertained to customer information relating to a loyalty programme and the related credit card (Pass card). The companies failed in their obligation to inform data subjects about data processing according to Art. 13 GDPR related to joining the loyalty programme or the Pass card. The information given was not easily accessible, easily understandable or complete. The companies also failed to adhere to French data protection law relating to cookies. The relevant websites installed advertising cookies without first obtaining the user's consent.

Carrefour France failed to comply with the obligation to limit the data retention period of its customers' personal data. It also infringed its obligation to facilitate the exercise of data subject rights and failed to respond to certain requests for access to personal data and deletion requests. Carrefour Banque infringed its obligation to process personal data fairly under Art. 5 GDPR as it processed more personal data than what it had indicated to people subscribing to the Pass card.

On all points, the companies changed their practices during the procedure and committed significant resources to make the necessary modifications to bring them into compliance with the GDPR.

On 7 December, the French SA fined the companies Google LLC and Google Ireland Ltd a total of EUR 100,000,000 for having placed advertising cookies on the computers of users of the search engine google.fr, without obtaining prior consent and without providing them with adequate information.

The French SA justified the fines with regard to the seriousness of the breach of the French Data Protection Act. It also highlighted the scope of the search engine Google Search in France and the fact that the practices of the companies affected almost 50 million users. It noted the companies generated significant profits deriving from the advertising income indirectly generated from data collected by the advertising cookies. The French SA noted that the companies had stopped automatically placing advertising cookies when a user arrived on the page google.fr after an update in September 2020. The French SA, however, noticed that the new information banner set up by the companies when a user arrived on the page google.fr still did not allow the users living in France to understand the purposes for which the cookies were used and did not let them know that they could refuse these cookies. As a consequence, in addition to the financial penalties, the French SA also ordered the companies to adequately inform individuals, in accordance with the French Data Protection Act, within three months of the notification of the decision. Failing that, the companies must pay a penalty payment of EUR 100,000 for each day of delay.

Similar to the Google enforcement action, on 7 December, the French SA fined Amazon Europe Core EUR 35,000,000 for having placed advertising cookies on users' computers from the page amazon.fr, both without obtaining their prior consent and without providing them with adequate information about the personal data processing. The amount of the fine, and the decision to make it public, were justified by the seriousness of the breaches observed.

The French SA noted recent developments made on the site amazon.fr and, in particular, the fact that now no cookie is placed before obtaining the user's consent. The new information banner set up, however, still did not allow the users living in France to understand that the cookies are mainly used to personalise advertisements. Moreover, users were still not informed that they could refuse these cookies. In addition to the financial penalty, the French SA also ordered the company to adequately inform individuals per the French Data Protection Act, within three months of the notification of the decision. Otherwise, the company must pay a penalty payment of EUR 100,000 for each day of delay.

6.2.1.10. Germany

Germany has both a national (federal) SA and regional SAs. Three noteworthy cases involved enforcement actions by regional German SAs. The Lower Saxony SA imposed a fine of EUR 65,500 on a pharmaceutical manufacturer for using unsuitable and outdated software components on its website, equating to inadequate technical measures for the protection of personal data and thus breaching Art. 32(1) GDPR. The Berlin SA imposed a fine of EUR 6,000 on the regional association of a right-wing political party (the data controller) for the unlawful publication of personal data. The Hamburg SA imposed a fine of EUR 35,258,708 on H&M for data protection violations.

6.2.1.11. Greece

In response to a complaint, the Hellenic SA conducted an investigation regarding the lawfulness of personal data processing on a server of the company ALLSEAS MARINE S.A. Specifically, the Hellenic SA investigation covered access

to and inspection by an employer of an employee's emails on a company server; the illegal installation and operation of a closed-circuit video-surveillance system; and infringement of the right of access. The Hellenic SA found that the company had a legal right under Art. 5(1) and Art. 6(1)(f) GDPR to carry out an internal investigation that involved searching and retrieving the employee's emails. It found, however, that the closed-circuit video-surveillance system had been installed and operated illegally and, in addition, the recorded material submitted to the Hellenic SA was considered illegal. Finally, the Hellenic SA concluded that the company did not satisfy the employee's right of access to his personal data contained in his corporate PC.

Furthermore, following a complaint to the Hellenic SA that Public Power Corporation S.A. (PPC) did not satisfy the data subject's right of access to information, the Hellenic SA issued an administrative fine of EUR 5,000 to the company. One month after receiving the request, PPC, as a data controller, did not provide a response to the complainant regarding the inability to immediately meet this right. Given the recurrence of a previous similar infringement by PPC, the Hellenic SA unanimously decided that an effective, proportionate and dissuasive administrative fine should be imposed.

In another case, the Hellenic SA examined a complaint against a special education centre for its failure to satisfy the right of access exercised by a father, on behalf of his child, in the exercise of parental responsibility. The controller had not complied with the Hellenic SA's initial request to immediately satisfy the applicant's right of access. The Hellenic SA issued an order to the controller to provide the requested documents to the complainant, including tax documents. It also imposed an administrative fine of EUR 3,000 on the controller for not satisfying this right.

6.2.1.12. Hungary

The Hungarian SA issued many fines during 2020. This section includes some examples of key cases.

On 28 May, the Hungarian SA issued a fine of HUF 100,000,000 to a telecommunications service provider for multiple GDPR infringements. The Hungarian SA initiated an investigation following a personal data breach of which the company notified the Hungarian SA within the 72-hour period set out by the GDPR. The incident was triggered by the unauthorised access to the company's database, which had been conducted and reported in good faith by an ethical hacker. The Hungarian SA established that the company infringed provisions in Art. 5 GDPR, pertaining to purpose limitation and storage limitation, by failing to erase a test database.

In July, the Hungarian SA imposed a total of HUF 4,500,000 in data protection fines on Mediarey Hungary Services Zrt., the publisher of the Hungarian Forbes magazine, in two cases. The fines pertained to the magazine failing to carry out a proper interest assessment. It also did not inform various data subjects, who appeared in a list of the 50 richest Hungarians, of the results of comparing its own legitimate interests with that of a third party (the public) and of the data subjects themselves. Forbes also failed to provide information to the data subjects about the circumstances of the data processing and their data subject rights.

On 3 September, a company distributing shoes was fined a total amount of HUF 20,000,000. The involved data subject alleged that he received the wrong change when buying a pair of shoes and requested that the company let him see the shop's video footage of the exchange, which they did not allow without a police warrant; the company eventually deleted the footage after the retention period expired. The company failed to give its reasons for not letting him view the recordings and refused to let him exercise his rights to access and the right to restrict processing.

6.2.1.13. Iceland

On 5 March, the Icelandic SA decided to impose an administrative fine of ISK 3,000,000 on the National Centre of Addiction Medicine (NCAM) in a case relating to a personal data breach. The breach occurred when a former employee of the NCAM received boxes containing what were supposed to be personal belongings that he had left there. It turned out, however, that the boxes also contained patient data, including health records of 252 former patients and records containing the names of approximately 3,000 people who had attended rehabilitation for alcohol and substance abuse. The Icelandic SA concluded that the breach was a result of the data controller's lack of implementation of appropriate data protection policies and appropriate technical and organisational measures to protect the data, which constituted a violation of the GDPR, so issued the fine.

In a similar case, also on 5 March, the Icelandic SA decided to impose an administrative fine of ISK 1,300,000 on the Breiðholt Upper Secondary School pertaining to a personal data breach. The breach occurred when a teacher at the school sent an e-mail to his students and their parents/guardians, attaching a document that he believed to contain information on consultation appointments. However, it contained data on the well-being, study performance and social conditions of a different group of students; some of the personal data was sensitive. The Icelandic SA concluded that the breach resulted from a lack of implementation of appropriate data protection policies and appropriate technical and organisational measures. As such, this amounted to a violation of the GDPR and warranted the fine.

6.2.1.14. Ireland

On 15 December, the Irish SA announced the conclusion of a GDPR investigation it had conducted into Twitter International Company (TIC). The Irish SA started its investigation in January 2019 following receipt of a breach notification from TIC. The Irish SA found that TIC had infringed Arts. 33(1) and 33(5) GDPR in failing to notify the Irish SA of the breach on time and failing to adequately document the breach. The Irish SA imposed an administrative fine of EUR 450,000 on TIC as an effective, proportionate and dissuasive measure.

The draft decision in this inquiry, having been submitted to other CSAs under Art. 60 GDPR in May, was the first one to go through the Art. 65 GDPR (dispute resolution) process since the introduction of the GDPR and was the first Draft Decision in a "big tech" case on which all EEA SAs were consulted as CSAs.

The EDPB has published the Art. 65 GDPR decision and the final Irish SA decision on its website.

6.2.1.15. Italy

The Italian SA imposed two fines on Eni Gas and Luce (Egl), totalling EUR 11,500,000, concerning respectively the illicit processing of personal data in the context of promotional activities and the activation of unsolicited contracts. The fines were determined in view of the parameters set out in the GDPR, including the wide range of stakeholders involved, the pervasiveness of the conduct, the duration of the infringement, and the economic conditions of Egl. The first fine of EUR 8,500,000 related to unlawful processing in connection with telemarketing and teleselling activities. The second fine of EUR 3,000,000 concerned breaches due to the conclusion of unsolicited contracts for the supply of electricity and gas under free market conditions.

The Italian SA fined TIM SpA (TIM) EUR 27,802,496 on account of several instances of unlawful processing for marketing purposes. Overall, the infringements concerned millions of individuals. TIM were proven to be insufficiently familiar

with fundamental features of the processing activities they performed, thus threatening accountability. In many cases out of the millions of marketing calls that had been placed in a six-month period with non-customers, the Italian SA could establish that the call centre operators relied upon by TIM had contacted the data subjects in the absence of any consent. Inaccurate, unclear data processing information was provided in connection with certain apps targeted at customers and the arrangements for obtaining the required consent were inadequate. The data breach management system also proved ineffective, and no adequate implementation and management systems were in place regarding personal data processing, which fell short of privacy by design requirements. As well as the fine, the Italian SA imposed 20 corrective measures on TIM, including both prohibitions and injunctions.

On 9 July, the Italian SA fined the telephone operators Wind Tre SpA and Iliad about EUR 17,000,000 and EUR 800,000, respectively. The Wind Tre SpA fine was issued on account of several instances of unlawful data processing that were mostly related to unsolicited marketing communications made without users' consent. Some users had been unable to withdraw consent or object to the processing of their personal data for marketing processes. The Italian SA had already issued a prohibitory injunction against the company on account of similar infringements that had occurred when the previous data protection law was in force. The other telephone operator, Iliad, had shown shortcomings in particular concerning employees' access to traffic data.

The Italian SA ordered Vodafone to pay a fine of more than EUR 12,250,000 on account of having unlawfully processed the personal data of millions of users for telemarketing purposes. As well as having to pay the fine, the company was required to implement several measures set out by the Italian SA to comply with national and EU data protection legislation.

Furthermore, pertaining to the private sector, the Italian SA made two decisions providing for corrective measures and administrative fines. Related to the public sector, the Italian SA issued 20 reprimands and 30 administrative fines without corrective measures. Significant cases involved municipalities, universities, health care organisations and schools.

6.2.1.16. Latvia

The Latvian SA imposed a fine of EUR 15,000 on one of the biggest online stores in Latvia (SIA "HH Invest"). The Latvian SA examined the content of the website's privacy policy, concluding that the information available to data subjects was not in easy-to-understand language and that information was provided in a non-systematic way. Furthermore, it was established that certain aspects of the processing that had to be explained to the data subject in accordance with Art. 13 GDPR were not clarified. The administrative fine was imposed taking into account the fact that the online store actively cooperated with the Latvian SA during the inspection and had remedied the non-compliance identified by the Latvian SA.

The Latvian SA also imposed a fine of EUR 6,250 on a company for the improper processing of employee personal data. The Latvian SA received a complaint about the actions of the employer in sending third persons (other employees) an e-mail containing information about the data subjects' names and health conditions, including diagnoses of infectious disease. After investigation, the Latvian SA found that the relevant personal data had been processed inappropriately because such processing was not necessary to achieve the employer's objectives and no legal basis under Art. 9 GDPR was applicable to such processing. When imposing a fine, the Latvian SA considered that the incident was an isolated incident and that no evidence was found that the company would do this systematically.

6.2.1.17. Lithuania

In 2020, the Lithuanian SA imposed multiple fines for GDPR violations. Most of the fines were imposed because of non-cooperation, where the organisations involved in the investigation did not provide the requested information to the Lithuanian SA.

In April, the Lithuanian SA carried out an investigation into sound recording in public transport buses. The Lithuanian SA fined the private company UAB "Vilniaus viešasis transportas" EUR 8,000 for violating Arts. 5, 13, 24 and 35 GDPR.

In September, the Lithuanian SA reprimanded the Vilnius City Municipality Administration for infringements of Arts. 5(1)(d) and 5(1)(f) GDPR. Specifically, the Municipality Administration had failed to implement appropriate technical and organisational measures, thereby failing to ensure the accuracy of personal data pertaining to the parents of an adopted child. The Lithuanian SA fined the Municipality Administration EUR 15,000.

6.2.1.18. The Netherlands

The Dutch SA imposed seven fines in 2020. Not all these fines have been made public, so the Dutch SA may not yet disclose the amount of the fines and other details. In addition to these fines, the Dutch SA issued one order subject to penalty and took a number of other corrective measures. Some cases are listed here:

- In February, the Dutch SA published an order subject to penalty directed at health insurance company CZ because the company processed too much medical data for the assessment of applications for reimbursement of rehabilitation care;
- In March, the Dutch SA fined the tennis association KNLTB EUR 525,000 for selling the personal data of its members;
- In April, the Dutch SA published a fine of EUR 725,000, imposed on a company that required employees to have their fingerprints scanned for time and attendance registration. Following an investigation, the Dutch SA concluded that the company was not authorised to process its employees' fingerprint data. The company was not entitled to invoke an exemption for processing sensitive personal data;
- In July, the Dutch SA imposed a fine of EUR 830,000 on the National Credit Register (BKR). The BKR had created too many obstacles for people wishing to access their data. Among other things, the BKR charged people who wished access to the personal data that the BKR had about them.

6.2.1.19. Norway

The Norwegian SA issued multiple fines in 2020. The Norwegian SA carried out the following actions:

- Imposed an administrative fine equivalent to EUR 18,870 on the Indre Østfold Municipality due to a breach of confidentiality, where personal data that should have been protected was made available to unauthorised persons;
- Reprimanded Telenor Norge AS for a lack of personal data security in a voice mailbox function, and for failing to notify the Norwegian SA of a data breach;
- Notified the Norwegian Institute of Public Health (NIPH) of its intention to impose a temporary ban on personal data processing in connection with the Smittestopp contact tracing mobile app. The NIPH temporarily suspended all use of the app. In August, the Norwegian SA reached a decision to temporarily ban the processing of personal data using the Smittestopp app as it could not be considered a proportionate intervention in a user's fundamental right to data protection. The NIPH had already decided to stop collecting personal data and to erase the collected data;
- Imposed an administrative fine equivalent to EUR 47,500 on the Rælingen Municipality after data concerning the health of children with special needs was processed using the digital learning platform Showbie;

- Issued the Norwegian Public Roads Administration a fine equivalent to EUR 37,400 for processing personal data for purposes that were incompatible with the originally stated purposes, and for not erasing video recordings after seven days;
- Made final a decision to issue an administrative fine to the Bergen Municipality equivalent to approximately EUR 276,000. This was in response to a data breach in October 2019 regarding the Municipality's new tool for communication between school and home. Personal information in the communication system was not secure enough;
- Issued Odin Flissenter AS with an administrative fine equivalent to EUR 13,905 for performing a credit check of a sole proprietorship without having a lawful basis for the processing;
- Decided on an administrative fee of NOK 750,000 for the Østfold HF Hospital. During the period from 2013 to 2019, the hospital stored report extracts from patient records that were not access controlled, so were stored in a non-secure manner. The case started with a personal data breach notification from the hospital. The Norwegian SA considered that the Østfold HF Hospital had not established a system for access control that was sufficient to prevent similar breaches from occurring in the future, and referred particularly to the routines for access control and personal data storage. The management system was required to involve follow-up that the routines are followed, which also means ensuring that only secure systems are used in the processing of sensitive personal data.

6.2.1.20. Poland

The President of the Polish SA imposed 11 administrative fines in 2020, some of which are listed vbelow:

- On 18 February, the Polish SA imposed a fine of PLN 20,000 (EUR 4,600) in connection with a breach consisting of the processing of the biometric data of children when using the school canteen without a legal basis;
- On 9 March, the Polish SA imposed a fine of PLN 20,000 (EUR 4,600) on Vis Consulting Sp. z o.o., a company from the telemarketing industry, for making it impossible to conduct an inspection;
- On 29 May, the Polish SA imposed a fine of PLN 15,000 (EUR 3,500) in cross-border proceedings on the East Power company from Jelenia Góra for failing to provide the Polish SA with access to personal data and other information necessary for the performance of its tasks;
- On 3 June, the Polish SA imposed a fine of PLN 5,000 (EUR 1,168) on an individual entrepreneur running a non-public nursery and pre-school for failing to provide the Polish SA with access to personal data and other information necessary for the performance of its tasks;
- On 2 July, the Polish SA imposed a fine of PLN 100,000 (EUR 23,000) on the Surveyor General of Poland for failing to provide the Polish SA with access to premises, data processing equipment and means, and access to personal data and information necessary for the Polish SA to perform its tasks during the inspection;
- In addition, on 24 August, the Polish SA imposed another fine of PLN 100,000 (EUR 23,000) on the Surveyor General of Poland for infringing the principle of lawfulness of personal data processing;
- On 21 August, the Polish SA imposed a fine on the Warsaw University of Life Sciences of PLN 50,000 (EUR 11,500) after having found a personal data breach;
- On 3 December, the Polish SA imposed a fine of PLN 1,900,000 million (EUR 460,000) on Virgin Mobile Polska for not implementing appropriate technical and organisational measures to ensure the security of the processed data;
- On 9 December, the Polish SA imposed a fine of over PLN 12,000 (EUR 3,000) on a Smart Cities company from Warsaw for not cooperating with the Polish SA;
- On 9 December, the Polish SA imposed a fine of PLN 85,588 (EUR 20,000) on WARTA S.A. Insurance and Reinsurance Company for failing to notify the President of the Polish SA of a personal data breach;

- On 17 December, the Polish SA imposed a fine of over PLN 1,000,000 (EUR 250,000) on the ID Finance Poland company for failing to implement appropriate technical and organizational measures.

6.2.1.21. Portugal

The Portuguese SA issued several corrective measures within its powers under Art. 58 GDPR. In one example, it compelled a controller in the field of market studies to delete a data subject's personal data.

In two cases, the Portuguese SA ordered two controllers and one processor, all in the public health sector, to bring data processing into compliance with the GDPR and to adopt specific measures to remedy the deficiencies found within the context of COVID-19 data processing. There were also two situations where the Portuguese SA issued an order to temporarily ban data processing until certain conditions were met. Both cases related to the collection by web cameras of images of people on the beach, which were transmitted online in real-time. The two different private data controllers had to take the appropriate technical measures to process images with no identifiable individuals.

The Portuguese SA also imposed a fine on a private company for violating the principle of lawfulness. Due to the COVID-19 pandemic, all sanction proceedings were suspended for four months, in accordance with national law. Therefore, although some proceedings were ongoing and controllers were already notified of a draft decision involving the application of fines, there were no more final decisions in 2020 regarding GDPR cases; they only pertained to ePrivacy cases.

6.2.1.22. Romania

In 2020, the Romanian SA conducted 21 enforcement measures for violations of the GDPR, as outlined here.

- On 13 January, the Romanian SA fined Hora Credit IFN S.A. the equivalent of EUR 14,000 for multiple GDPR violations and issued various corrective measures to ensure compliance with the GDPR;
- On 14 January, the Romanian SA sanctioned SC Enel Energie S.A with two fines amounting to the equivalent of EUR 6,000 for violating provisions within Arts. 5, 6, 7 and 21 GDPR;
- On 25 March, the Romanian SA imposed several administrative fines and corrective measures on three data controllers. The controller Dante Internațional SA was sanctioned with an administrative fine of the equivalent of EUR 3,000; the controller Association "SOS Infertilitatea" with the equivalent of EUR 2,000; and the controller Vodafone România SA with the equivalent of EUR 4,100;
- On 31 March, the Romanian SA fined Vodafone România the equivalent of EUR 3,000 for violating Art. 5 GDPR and imposed corrective measures to ensure its compliance with the GDP;
- On 11 June, the Romanian SA imposed two fines: controller Estee Lauder Romania SRL was sanctioned with a fine equivalent to EUR 3,000 for unlawful data processing and the controller Telekom Romania Communications SA was fined the equivalent of EUR 3,000 for not implementing sufficient security measures;
- On 18 June, the Romanian SA found that Enel Energie Muntenia SA did not implement sufficient security and confidentiality measures to prevent the accidental disclosure of personal data to unauthorised persons and fined them the equivalent of EUR 4,000;
- On 9 July, the Romanian SA found that Proleasing Motors SRL had violated Art. 32 GDPR and subsequently fined them the equivalent of EUR 15,000;
- On 27 July, the Romanian SA fined SC CNTAR TAROM SA the equivalent of EUR 5,000 and imposed a corrective measure to ensure the controller reviewed and updated the technical and organisational measures it had in place;

- On 30 July, the Romanian SA imposed two fines. First, it fined S.C. Viva Credit IFN S.A. the equivalent of EUR 2,000 and imposed corrective measures. Second, it fined controller Compania Națională Poșta Română the equivalent of EUR 2,000;
- On 1 September, the Romanian SA sanctioned the Owners' Association Block FC 5, Năvodari city, Constanța county with a fine equivalent to EUR 500; it reprimanded the Owners' Association for failing to adhere to certain provisions in the GDPR; and imposed certain corrective measures;
- On 8 September, the controller Sanatatea Press Group S.R.L. was sanctioned with a fine equivalent to EUR 2,000 for not adhering to data security measures;
- On 1 October, the Romanian SA fined Megareduceri TV S.R.L. the equivalent of EUR 3,000 and fined the Owners' Association Militari R, Chiajna village the equivalent of EUR 2,000 and imposed a corrective measure;
- On 15 October, the controller S.C. Marsorom S.R.L. was sanctioned with a fine equivalent to EUR 3,000;
- On 20 October, the Romanian SA fined controller Globus Score SRL the equivalent of EUR 2,000 for failing to fulfil an earlier corrective measure and imposed another corrective measure;
- On 23 November, the Romanian SA fined Vodafone România S.A. the equivalent of EUR 4,000 for not responding to data subject access and erasure requests, and issued a corrective measure;
- On 24 November, the Romanian SA issued a fine equivalent to EUR 5,000 to DADA CREATION S.R.L. for violating Art. 32 GDPR and reprimanded the controller for infringing Art. 33 GDPR. The Romanian SA also issued a corrective measure.

6.2.1.23. Slovakia

The Slovak SA fined a primary school EUR 6,000 for breaching the principle of lawfulness, principle of accountability and for the failure to comply with its obligation to handle the data subjects' requests to an adequate extent.

6.2.1.24. Slovenia

The Slovenian SA often deals with cases regarding unlawful video surveillance in work areas. There are some specific provisions on video surveillance permissibility in national law, in addition to the GDPR provisions. In one such case, the Slovenian SA did not permit video surveillance as a means for an employer to constantly monitor the work process by using an app on his mobile phone. According to national law, video surveillance within work areas may only be implemented in exceptional cases when it is necessarily required for the safety of people or property, or to protect secret data and business secrets.

An individual exercised his right to rectification regarding his financial information in SISBON, which is a Slovenian information system on credit ratings that is designed for mutual exchange and processing of data on natural persons. The Bank of Slovenia manages SISBON, and all the banks and most of the financial subjects are required to provide information to the system. The individual's demand to rectify the information had been denied by the data controller (bank). Later, the primary bank was no longer technically able to rectify the data for the subject. The new creditor was not a member of SISBON and could not rectify the data. The Slovenian SA decided that the data controller violated the individual's right to rectification under the GDPR and that technical rules on managing the system should enable individuals to exercise this right.

A parish was processing the application of an individual on the right of erasure. The individual requested his personal data be erased from the register of births because he was no longer a member of the church. The Slovenian SA agreed with the position of the church, confirming that the register is an archive document, and the individual may not claim the right to erasure when the processing is needed for archiving purposes in the public interest.

The national health insurance fund was sending professional cards to users by mail and with personal data printed on the envelope (the insurance number, the barcode and the summary of the consignment). The Slovenian SA ordered the data processor to restrict the listing of the personal data on the envelope.

6.2.1.25. Spain

The Spanish SA fined the company Iberdrola EUR 4,000 for not responding to its request for information. In short, Iberdrola had not provided the information required and consequently hindered the investigative powers that each Spanish SA has, thereby infringing Art. 58(1) GDPR.

The Spanish SA issued a fine of EUR 1,200 to a company for calling the data subject and offering him/her a deal on hotels, while he/she was in an advertisement exclusion system. By joining this system, the data subject had exercised his/her right to object to processing for marketing purposes under Art. 21 GDPR. The company, however, did not comply with its obligation to consult the advertisement exclusion system before making a telephone call with marketing purposes to avoid processing certain individuals' personal data.

The Spanish SA also fined Vodafone España EUR 75,000 for processing a claimant's telephone number for marketing purposes after the claimant had exercised the right to erasure in 2015, in spite of which the data subject was sent advertising messages. The controller stated that the claimant number, being easy to remember, had been used as a "dummy number" by its employees.

The Spanish SA imposed also a fine of EUR 70,000 on Xfera Móviles for disclosing a customer's personal data to a third party. The SA issued a fine of EUR 75,000 to Telefónica Móviles España, S.A.U. for unlawfully processing a claimant's personal data by charging the claimant several invoices corresponding to a third person.

6.2.1.26. Sweden

The Swedish SA issued multiple fines in 2020. The Swedish SA carried out these enforcement acts:

- Imposed an administrative fine of SEK 75,000,000 on Google for failing to comply with the GDPR. As a search engine operator, it had not fulfilled its obligations in respect to the right to request delisting;
- Issued a fine of SEK 200,000 to the National Government Service Centre for failing to notify affected parties as well as the Swedish SA about a personal data breach in due time;
- In response to a complaint, conducted an investigation that showed that the Healthcare Committee in Region Örebro County made a mistake when publishing sensitive personal data about a patient admitted to a forensic psychiatric clinic on the region's website. The Swedish SA ordered the Committee to bring its personal data handling into compliance with the GDPR and furthermore issued an administrative fine of SEK 120,000 against the Committee;
- Investigated the use by a co-operative housing association of video surveillance on its property. It concluded that the association had gone too far when using video surveillance in the main entrance and stairwell, and when recording audio. The Swedish SA ordered the co-operative housing association to stop these specific surveillance activities and to improve the information provided concerning the video surveillance. Furthermore, it issued an administrative

fine of SEK 20,000 to the association. When calculating the amount of the fine, the Swedish SA considered the fact that it was a smaller co-operative housing association;

- Reviewed the so-called School Platform, which is the IT system used, among other things, for student administration of schools in the City of Stockholm. The review showed an insufficient level of security of such a grave nature that the Swedish SA issued an administrative fine of SEK 4,000,000 to the Board of Education in the City of Stockholm;
- Received a complaint from the relative of a resident of a residential care home for persons with certain functional impairments (so-called LSS housing) in Gnosjö Municipality, claiming that the resident was being monitored illegally. The Swedish SA initiated an audit of the LSS housing and concluded that the resident in question was indeed monitored in his/her bedroom in violation of the GDPR and the Swedish Video Surveillance Act. In its decision, the Swedish SA stated that there was no legal basis for the video surveillance, that an Impact Assessment had not been carried out before initiating the video surveillance and that the controller had failed to clearly inform the resident about the video surveillance. For these reasons, the Swedish SA issued an administrative fine of SEK 200,000 to the Social Welfare Committee;
- Audited eight health care providers in how they governed and restricted personnel's access to the main systems for electronic health records. The Swedish SA discovered insufficiencies that in seven of the eight cases lead to administrative fines of up to SEK 30,000,000;
- Issued a fine of SEK 550,000 against the Umeå University for failing to sufficiently protect sensitive personal data. Specifically, the University had processed special categories of personal data concerning sexual life and health through, amongst others, storage on a cloud service, without sufficiently protecting the data;
- Imposed an administrative fine of SEK 300,000 on a housing company for unlawful video surveillance in an apartment building.

6.3. SURVEY – BUDGET AND STAFF

In the context of the evaluation of the GDPR, the EDPB conducted a survey among the SAs about their budget and staff. Based on information provided by SAs from 30 EEA countries before February 2020, an increase in the budget for 2020 was envisaged in 26 cases. In respect of the remaining four SAs, three forecasted no change and for one no data was available. According to the same survey, a majority of SAs (23) anticipated an increase in staff numbers in 2020. Five SAs forecast that the number of their employees would not increase from 2019 to 2020, while two SAs predicted a decrease in staff numbers. Differences in personnel requirements across SAs are to be expected, given the varied remits of the SAs.

In its contribution to the evaluation of the GDPR, the EDPB stresses that the effective application of the powers and tasks attributed by the GDPR to SAs is largely dependent on the resources available to them. Even though most SAs reported an increase in staff and resources, a majority of the SAs stated that resources made available to them were insufficient. The EDPB noted that this applies, in particular, to the OSS mechanism, as its success depends on the time and effort that SAs can dedicate to individual cases and cooperation.

7

Coordinated Supervision Committee of the large EU Information Systems and of EU bodies, offices and agencies

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

To ensure the consistency of supervision efforts on both levels, all SAs involved, including the EDPS, used to cooperate through Supervision Coordination Groups (SCGs). Each of these groups was dedicated to a specific EU database.

Since December 2018, Regulation 2018/1725 has provided for a single model of coordinated supervision for large-scale EU IT systems and agencies within the framework of the EDPB. This replaces the current system of individual SCGs. The new model does not apply to all EU information systems and agencies at once, but progressively, according to when the revised version of the establishing act of each EU information system and agency becomes applicable.

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

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

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

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

Internal Market:

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

Police and Judicial Cooperation:

- Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States.

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

Border, Asylum and Migration:

- Schengen Information System (SIS), ensuring border control cooperation (before the end of 2021);
- Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen States (expected in 2022);
- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone (expected in 2022);
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States (expected in 2023);
- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State;
- Customs Information System (CIS), which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation.

Police and Judicial Cooperation:

- SIS, which also ensures law enforcement cooperation (before the end of 2021);
- European Public Prosecutor Office (EPPO) (before the end of 2021);
- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked (expected for 2022);
- Europol, the EU's law enforcement agency (expected by end of 2021 or early 2022).

8

Main objectives for 2021

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

8.1. 2021-2023 STRATEGY

The EDPB defined its Strategy for 2021-2023, which covers the four main pillars of its strategic objectives, as well as a set of three key actions per pillar to help achieve these objectives.

The pillars and key actions are as follows:

1. Advancing **harmonisation** and facilitating **compliance** by:
    a. Providing guidance on key notions of EU data protection law;
    b. Promoting development and implementation of compliance mechanisms for data controllers and processors;
    c. Fostering the development of common tools for a wider audience and engaging in awareness raising and outreach activities.

2. Supporting **effective enforcement** and **efficient cooperation between national SAs** by:

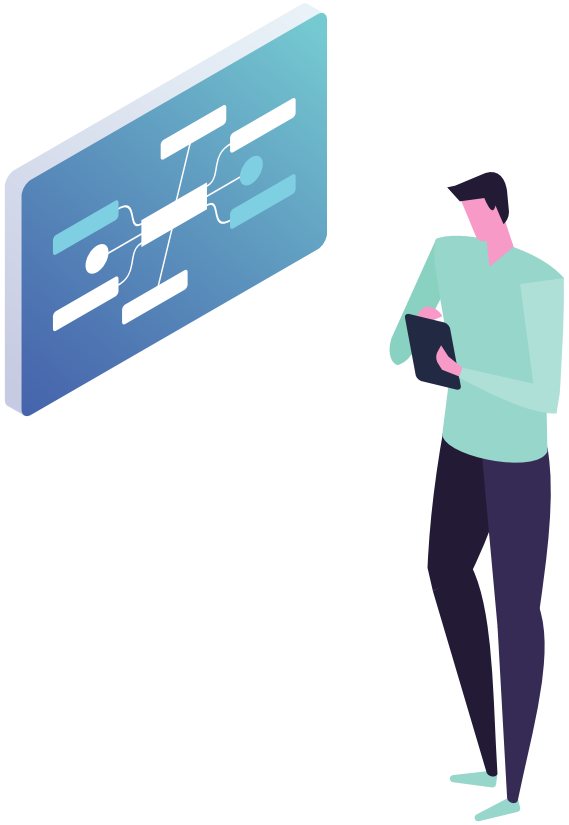
    a. Encouraging and facilitating use of the full range of cooperation tools enshrined in Chapter VII GDPR and Chapter VII Law Enforcement Directive;
    b. Implementing a Coordinated Enforcement Framework (CEF) to facilitate joint actions;
    c. Establishing a Support Pool of Experts (SPE).

3. Promoting **a fundamental rights approach to new technologies** by:

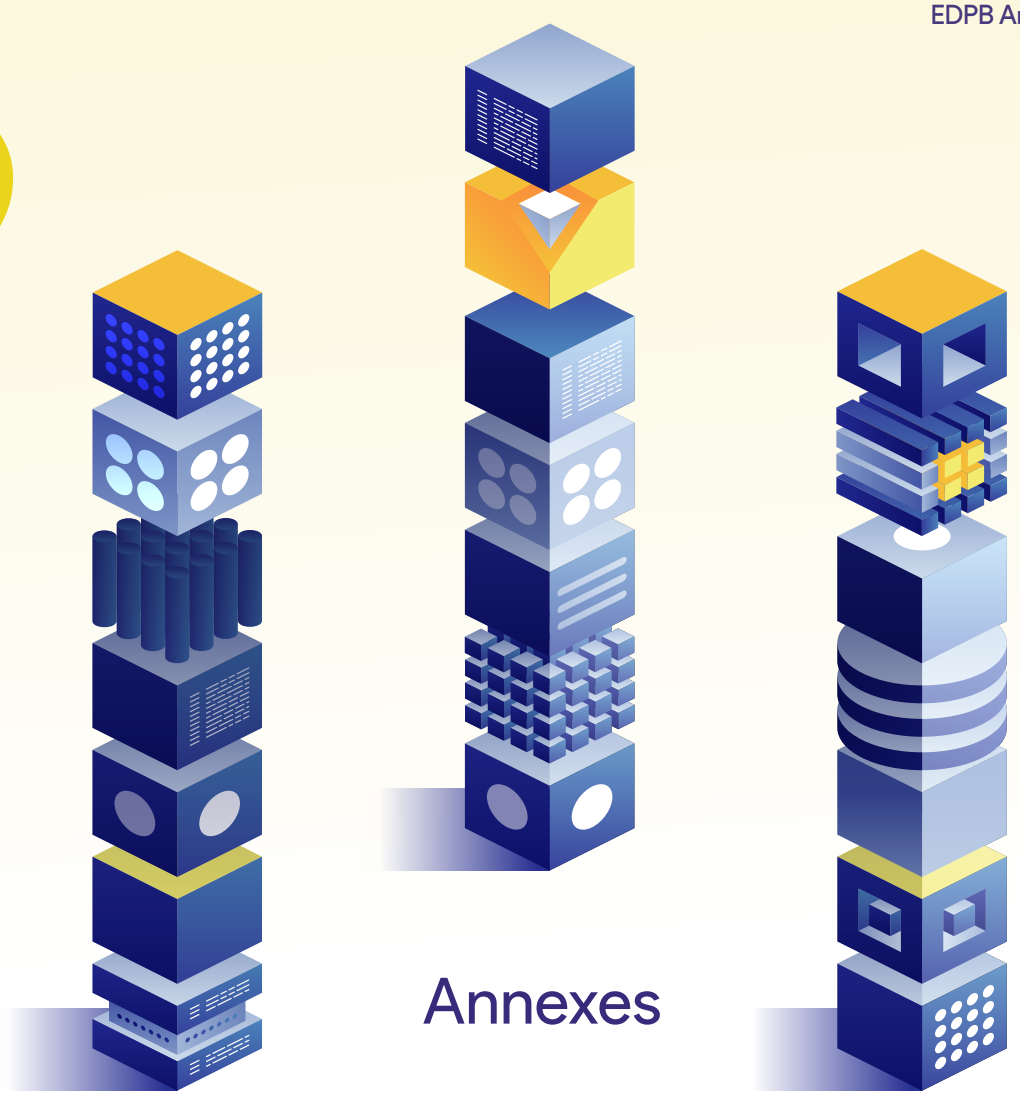
    a. Assessing those technologies;
    b. Reinforcing data protection by design and by default and accountability;
    c. Intensifying engagement and cooperation with other regulators and policymakers.

4. Advancing **a global dimension** by:

    a. Promoting and increasing awareness of the use and implementation of transfer tools which ensure a level of protection equivalent to the EEA;
    b. Engaging with the international community;
    c. Facilitating the engagement between the EDPB Members and the SAs of third countries with a focus on cooperation in enforcement cases involving controllers or processors located outside the EEA.



9



Annexes

9.1. GENERAL GUIDANCE ADOPTED IN 2020

- Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications
- Guidelines 02/2020 on Arts. 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies
- Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
- Guidelines 05/2020 on consent under Regulation 2016/679
- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR - Adopted after public consultation
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- Guidelines 08/2020 on the targeting of social media users
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679
- Guidelines 10/2020 on restrictions under Art. 23 GDPR
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - version for public consultation
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

9.2. CONSISTENCY OPINIONS ADOPTED IN 2020

- Opinion 01/2020 on the Spanish data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 02/2020 on the Belgium data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 03/2020 on the France data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 04/2020 on the draft decision of the competent Supervisory Authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 05/2020 on the draft decision of the competent Supervisory Authority of Luxembourg regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 06/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Fujikura Automotive Europe Group (FAE Group)
- Opinion 07/2020 on the draft list of the competent Supervisory Authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Art. 35(5) GDPR)
- Opinion 08/2020 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Reinsurance Group of America
- Opinion 09/2020 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of Reinsurance Group of America
- Opinion 10/2020 on the draft decision of the competent Supervisory Authorities of Germany regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 11/2020 on the draft decision of the competent Supervisory Authority of Ireland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 12/2020 on the draft decision of the competent Supervisory Authority of Finland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 13/2020 on the draft decision of the competent Supervisory Authority of Italy regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 14/2020 on the draft decision of the competent Supervisory Authority of Ireland regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 15/2020 on the draft decision of the competent Supervisory Authorities of Germany regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 16/2020 on the draft decision of the competent Supervisory Authority of the Czech Republic regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the Slovenian Supervisory Authority (Art. 28(8) GDPR)
- Opinion 18/2020 on the draft decision of the competent Supervisory Authority of the Netherlands regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR

- Opinion 19/2020 on the draft decision of the competent Supervisory Authority of Denmark regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 20/2020 on the draft decision of the competent Supervisory Authority of Greece regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 21/2020 on the draft decision of the competent Supervisory Authority of the Netherlands regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 22/2020 on the draft decision of the competent Supervisory Authority of Greece regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 23/2020 on the draft decision of the competent supervisory authority of Italy regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 24/2020 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of Jotun
- Opinion 25/2020 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Tetra Pak
- Opinion 26/2020 on the draft decision of the competent Supervisory Authority of Denmark regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 27/2020 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Coloplast Group
- Opinion 28/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Iberdrola Group
- Opinion 29/2020 on the draft decision of the Lower Saxony Supervisory Authority regarding the Controller Binding Corporate Rules of Novelis Group
- Opinion 30/2020 on the draft decision of the competent Supervisory Authority of Austria regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 31/2020 on the draft decision of the competent Supervisory Authority of Poland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 32/2020 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of Equinix

9.3. LEGISLATIVE CONSULTATION

- EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic — 14/04/2020
- Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB - 19/11/2020

9.4. OTHER DOCUMENTS

- Contribution of the EDPB to the evaluation of the GDPR under Art. 97 - 18/02/2020
    - Individual replies from the data protection supervisory authorities
- Statement on privacy implications of mergers – 19/02/2020
- Statement on the processing of personal data in the context of the COVID-19 outbreak — 19/03/2020

- Mandate on the processing of health data for research purposes in the context of the COVID-19 outbreak — 07/04/2020
- Mandate on geolocation and other tracing tools in the context of the COVID-19 outbreak — 07/04/2020
- Statement on restrictions on data subject rights in connection to the state of emergency in Member States — 02/06/2020
- Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak - 16/06/2020
- Statement on the data protection impact of the interoperability of contact tracing apps - 16/06/2020
- Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems - 17/07/2020
- Information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA - 22/07/2020
- Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems - 24/07/2020
- EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 - 20/10/2020
- Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing - 15/12/2020
- EDPB Document on Terms of Reference of the EDPB Support Pool of Experts - 15/12/2020
- Information note on data transfers under the GDPR to the United Kingdom after the transition period - 15/12/2020
    - Superseded by Information note on data transfers under the GDPR to the United Kingdom after the transition period - 13/01/2021
- Statement on the end of the Brexit transition period - 15/12/2020
    - Superseded by Statement on the end of the Brexit transition period - 13/01/2021
- Pre-GDPR BCRs overview list - 21/12/2020

9.5. LIST OF EXPERT SUBGROUPS WITH SCOPE OF MANDATES

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
Borders, Travel & Law Enforcement (BTLE) Expert Subgroup	• Law Enforcement Directive • Cross-border requests for e-evidence • Adequacy decisions, access to transferred data by law enforcement and national intelligence authorities in third countries (e.g. follow-up to CJEU Schrems II judgment and draft EU adequacy decisions on the UK) • Passenger Name Records (PNR) • Border controls
Compliance, e-Government and Health (CEH) Expert Subgroup	• Codes of conduct, certification and accreditation • 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 • Compliance with public law and eGovernment • Health • Processing of personal data for scientific research purposes
Cooperation Expert Subgroup	• General focus on procedures of the GDPR • Guidance on procedural questions • 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

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
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
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 (e.g. ESMA) • 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

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
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

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
Strategic Advisory Expert Subgroup	• Guidance on strategic questions affecting the whole EDPB (including the discussion 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 • Geolocation and other tracing tools in the context of the COVID-19 outbreak

Contact details

Postal address

Rue Wiertz 60, B-1047 Brussels

Office address

Rue Montoyer 30, B-1000 Brussels

edpb

European Data Protection Board