2019 ANNUAL REPORT

WORKING TOGETHER FOR STRONGER RIGHTS

edpb
European Data Protection Board

European Data Protection Board
2019 Annual Report

WORKING TOGETHER FOR STRONGER RIGHTS

An Executive Summary of this report, which provides an overview of key EDPB activities in 2019, is also available.

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

EDPB Annual Report 2019

TABLE OF CONTENTS

Foreword

The European Data Protection Board's (EDPB) mission is to ensure the consistent application of data protection rules across the European Economic Area (EEA). This is enshrined in the General Data Protection Regulation (GDPR), which has opened the door to a new era of respect for data subject rights.

The GDPR is not just valuable insofar as it has established a harmonised legal framework for data protection across the EEA – one that has expanded and strengthened national data protection authorities' powers. The GDPR's entry into force has also encouraged greater awareness of data protection rights among individuals and organizations alike. This is more important than ever, given the increasing presence of data-dependent technologies in almost every facet of our lives.

As we approach the two-year anniversary of the GDPR's entry into application, I am convinced that the cooperation between EEA DPAs will result in the emergence of a common data protection culture. Some challenges remain, but the EDPB is working on solutions to overcome these and to make sure that the key cooperation procedure concepts are applied consistently.

As the EDPB, we contribute to the consistent interpretation of the GDPR by adopting Guidelines and Opinions. In 2019, we adopted five new Guidelines on topics such as privacy by design and default, and the right to be forgotten, as well as two Guidelines in their final, post-consultation versions. We also adopted 16 Consistency Opinions covering, among other topics, Data Protection Impact Assessments, accreditation requirements for code of conduct monitoring bodies, and the interplay between the ePrivacy Directive and the GDPR.

This was possible thanks to the consistent efforts of all actors within the EDPB, as well as the increased input and engagement from our stakeholders via events, workshops and surveys.

As we look forward to the coming year, we feel ready to tackle the outstanding items in our two-year working programme. We will continue to adopt guidance, to promote the cooperation on cross-border enforcement, and to advise the EU legislator on data protection issues.

More and more countries outside the EU are adopting data protection legislation. In doing so, they often base their legislation on the fundamental principles of the GDPR. I am confident that, in a not too distant future, we will see the protection of data subject rights become a global norm. This will lay the foundation for more secure data flows and increased transparency, as well as improved trust in the rule of law.

Andrea Jelinek
Chair of the European Data Protection Board

2

Mission statement, tasks and principles

The European Data Protection Board (EDPB) aims to ensure the consistent application of the General Data Protection Regulation (GDPR) and of the European Law Enforcement Directive across the European Economic Area (EEA).

The EDPB can adopt general guidance to further clarify European data protection laws, giving stakeholders, including individuals, a consistent interpretation of their rights and obligations as well as providing Supervisory Authorities (SAs) with a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Decisions (more precisely, 'Consistency Opinions' or 'Consistency Decisions') to guarantee a consistent application of the GDPR by SAs across the EEA.

The EDPB acts in accordance with its rules of procedure and guiding principles.

2.1. TASKS AND DUTIES

- The EDPB **provides** general guidance (including guidelines, recommendations and best practices) to clarify the law.
- The EDPB issues **Consistency** Opinions or Decisions to guarantee the consistent application of the GDPR by the EEA SAs.
- The EDPB promotes **cooperation** and the effective exchange of information and best practices between national SAs.
- The EDPB **advises** the European Commission on any issue related to the protection of personal data and new proposed legislation in the European Union.

2.2. GUIDING PRINCIPLES

- **Independence and impartiality.** The EDPB is an independent body, which performs its tasks and exercises its powers impartially.
- **Good governance, integrity and good administrative behaviour.** The EDPB acts in the public interest as an expert, trustworthy and authoritative body in the field of data protection, with good decision-making processes and sound financial management.
- **Collegiality and inclusiveness.** The EDPB is organised and acts collectively as a collegiate body, as established by the provisions of the GDPR and the European Law Enforcement Directive.
- **Cooperation.** The EDPB promotes cooperation between SAs and endeavours to operate by consensus wherever possible, holding the GDPR and the European Law Enforcement Directive as an overarching reference.
- **Transparency.** The EDPB carries out its work as openly as possible, so as to be more effective and more accountable to the public. The EDPB strives to explain its activities using clear language that is accessible to all.
- **Efficiency and modernisation.** The EDPB makes every effort to ensure that its work is as efficient and as flexible as possible, in order to achieve the highest level of cooperation between its members. The EDPB does this by using new technologies to keep working methods up to date, minimise formalities, and provide efficient administrative support.
- **Proactivity.** The EDPB undertakes its own initiatives, in order to anticipate and support innovative solutions that will help overcome digital challenges to data protection. The EDPB encourages the effective participation of stakeholders (whether members, observers, staff or invited experts), so that their needs and aspirations can be fully taken into account.

3

About the European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Economic Area (EEA) and promotes cooperation between the EEA Supervisory Authorities (SAs).

The EDPB is composed of representatives of the SAs and the European Data Protection Supervisor (EDPS). The SAs of the EEA EFTA (European Free Trade Association) States (Iceland, Liechtenstein and Norway) are also members with regard to GDPR-related matters, although they do not hold the right to vote, nor can they be elected as Chair or Deputy Chair of the EDPB.

The EDPB was established by the General Data Protection Regulation (GDPR). The European Commission and – with regard to GDPR-related matters – the EFTA Surveillance Authority have the right to participate in the activities and meetings of the EDPB without voting rights.

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

4

2019 – an overview

4.1. FUNCTIONING OF THE EDPB: REVISED RULES OF PROCEDURE

The Rules of Procedure (RoP) were adopted during the first plenary meeting of the EDPB on 25 May 2018. These outline the EDPB's most important operational rules, describing:

- The EDPB's guiding principles;
- The organisation of the EDPB;
- The cooperation between the EDPB members;
- The election of the Chair and the Deputy Chair of the EDPB;
- The EDPB's working methods.

In 2019, the EDPB adopted revised wording for Articles 8, 10, 22 and 24 of its RoP. The EDPB also adopted a new Article 37 RoP establishing a Coordinated Supervision Committee in the context of data processing by large information systems in use within the EU institutions, as well as by EU bodies, offices and agencies.

4.1.1. Article 8 RoP: Observers

Article 8 RoP outlines the possibility for the EDPB to have observers. In 2019, new wording was adopted to clarify the requirements for a non-EU country's data protection authority to be granted observer status.

4.1.2. Article 10 RoP: Opinions of the Board under Article 64 GDPR

The revision of Article 10 RoP clarified the procedure that follows the adoption of a Consistency Opinion under Article 64 GDPR.

The adopted changes ensure that all EDPB members will be informed whether an SA intends to maintain or amend its draft decision following the EDPB's Opinion.

In addition, the EDPB Secretariat, the rapporteurs and the expert subgroup members who prepared the Opinion will inform the EDPB members and the European Commission about how, in their view, the SA's amended decision takes into account the EDPB's Opinion. This provides both the EEA SAs and the EDPB with valuable feedback and enables them to exercise their rights under Article 65.1.c GDPR.

The revised article also encompasses any situation where an SA indicates to the EDPB Chair that it will not follow the Opinion of the EDPB, whether in part or as a whole. In this case, the RoP enable the Chair and the Deputy Chairs of the EDPB to refer the matter to the EDPB under Article 65.1.c GDPR. This does not, however, affect the right of any other concerned SA, of the European Commission or of the EFTA Surveillance Authority to refer the matter to the EDPB for an Article 65 GDPR decision procedure.

Finally, the revised article makes clear that the EDPB will not adopt any Opinion or any other position in the context of the same Article 64 GDPR procedure, e.g. to confirm that the amended draft decision is in line with the adopted Opinion.

4.1.3. Article 22 RoP: Voting procedure

In the updated version of the RoP, the EDPB clarified the voting procedures relating to its plenary meetings.

In particular, all votes on the final adoption of documents should be counted from the total number of EDPB members entitled to vote, regardless of whether they are present for the actual vote or not.

4.1.4. Article 24 RoP: Written voting procedure

Revised Article 24 RoP raised the threshold necessary for the suspension of written procedures decided by the Chair of the EDPB. According to the new text, at least three entitled-to-vote EDPB members are needed to request a suspension of the written procedure decided by the Chair of the EDPB.

In addition, the Chair of the EDPB will be able to suspend the written procedure decided by the EDPB upon the request of one EDPB member only if new circumstances that may substantially affect the outcome of the procedure arise.

The EDPB updated Rules of Procedure establish a Coordinated Supervision Committee and clarify the role of observers and voting procedures.

4.1.5. Article 37 RoP: Establishing the Coordinated Supervision Committee

In October 2018, Regulation 2018/1725 on the protection of personal data processed by the EU institutions and bodies was adopted. In accordance with Article 62 of this regulation, the European Data Protection Supervisor (EDPS) and the national SAs shall cooperate actively to ensure effective supervision of large-scale IT systems and of Union bodies, offices and agencies. As a result, the Coordinated Supervision Committee was created.

Consequently, the EDPB's RoP were amended to include a new Article 37, which formally establishes the Coordinated Supervision Committee within the EDPB. This Committee includes representatives from national SAs, the EDPS, and the SAs of non-EU Schengen Member States, when foreseen under EU law. The Rules of Procedure make clear that the participation in the Committee may differ from the EDPB's membership and participation. (For more information on the Committee, see Section 7.)

Article 37 RoP takes a horizontal and flexible approach to ensure consistent application and structure for the coordinated supervision of various EU information systems. The article establishes that the Committee functions autonomously with respect to the EDPB's activities, adhering to its own rules of procedure and working methods. The Secretariat of the Committee is provided by the EDPB Secretariat.

Article 37 RoP also requires the Committee to meet at least twice a year and to submit a joint report on coordinated supervision activities to the European Parliament, the European Council and the European Commission.

4.2. THE EDPB SECRETARIAT

The EDPB Secretariat ensures that all of the EDPB's activities comply with the legal framework applicable to the EDPB as an EU body and with its RoP. It is the main drafter for Consistency Opinions and Decisions, and serves as an institutional memory, ensuring documents' consistency over time. The role of the EDPB Secretariat is also to facilitate the EDPB's fair and effective decision-making and to act as a gateway for clear and consistent communication.

As outlined in the GDPR, the EDPB Secretariat is provided by the EDPS, which is a member of the EDPB, and is required to perform all its tasks exclusively under the instructions of the Chair of the EDPB. The EDPB Secretariat deals with a range of tasks, from drafting legal documents to handling media relations and organizing meetings.

As part of its support activities, the EDPB Secretariat has developed IT solutions to enable effective and secure communication between the EDPB members, including the Internal Market Information System (IMI). It has also set up a network of communications officers within the SAs, to develop and implement shared communication on EDPB news, information campaigns and communication tools.

Finally, the EDPB Secretariat assists the Chair in preparing for and presiding over the plenary meetings, as well with her speaking engagements.

4.3. COOPERATION AND CONSISTENCY

Under the GDPR, EEA Member States' SAs cooperate closely to ensure that individuals' data protection rights are protected consistently across the EEA. One task is to assist one another and coordinate decision-making in cross-border data protection cases.

Via the so-called cooperation and consistency mechanism, the EDPB issues Consistency Opinions or Decisions. In 2019, the EDPB adopted several Opinions and Guidelines (outlined in Section 5 of this report) to clarify fundamental provisions of the GDPR and to ensure consistency in its application among SAs.

The EDPB can also issue legally binding Consistency Decisions, for instance aiming to arbitrate if and when national SAs take different positions in cross-border cases.

SAs identified certain challenges when implementing the cooperation and consistency mechanism. In particular, the patchwork of national procedural laws was found to have an impact on the cooperation mechanism, due to differences in complaint handling procedures, position of the parties in the proceedings, admissibility criteria, duration of proceedings, deadlines, etc.

In addition, SAs' effective application of the powers and tasks attributed to them by the GDPR depends largely on the resources they have available. This applies in particular to the One-Stop-Shop (OSS) mechanism, the success of which is contingent on the time and effort SAs can dedicate to individual cases and cooperation.

Despite these challenges, the EDPB is convinced that the cooperation between SAs will result in a common data protection culture and consistent monitoring practices. One single set of rules has proved to be advantageous for data controllers and processors within the EEA, having brought greater legal certainty. It has also benefitted individuals who have seen their data subject rights reinforced.

The EDPB also promotes the cooperation between the EEA SAs in their task. The EDPB Secretariat provides logistical

support to some types of national cooperation taking place before any formal involvement of the EDPB. This will be applicable for the cooperation between SAs in case a competent SA prepares Binding Corporate Rules (BCR), Codes of Conduct or Certification Criteria.

The EDPB, upon the initiative of the EDPS, has also launched a secondment programme enabling staff exchanges between the EEA SAs and the EDPS, including the EDPB Secretariat.

4.3.1. IT communications tool (IMI)

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

IMI is a system developed by the European Commission's Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW). It was adapted to cater for the needs of the GDPR, in close cooperation with the EDPB Secretariat and the SAs. Upon its adoption, IMI has immediately proved to be an asset for SAs, which have since accessed and used the system on an almost daily basis.

To ensure that the IMI system is adapted to the changing needs of SAs, the EDPB created a dedicated expert subgroup which discusses and validates any necessary changes (i.e. a new workflow for the EDPB written procedure, available reports for different procedures, change of bilateral workflow of the information mutual assistance request into multilateral etc.). Additionally, the EDPB IMI Helpdesk has been created within the EDPB Secretariat, with dedicated staff providing day-to-day assistance to users.

Since the entry into application of the GDPR until the end of 2019, 807 cases were registered in the IMI system by the EEA SAs. From the case register, different procedures were initiated:

- Identification of the Lead Supervisory Authority (LSA) and Concerned Supervisory Authorities (CSA): 1,346 procedures.
- Mutual Assistance Procedures: 115 formal procedures and 2427 informal procedures.
- OSS: 142 draft decisions, out of which 79 resulted in final decisions.

5

European Data Protection Board activities in 2019

The EDPB aims to ensure the consistent application of the General Data Protection Regulation (GDPR) and of the European Law Enforcement Directive across the European Economic Area (EEA).

The EDPB can adopt general guidance to clarify European data protection laws. This provides the public and stakeholders with a consistent interpretation of their rights and obligations, and ensures that Supervisory Authorities (SAs) have a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Binding Decisions to guarantee the consistent application of the GDPR by national SAs.

5.1. GENERAL GUIDANCE

In 2019, the EDPB adopted five new Guidelines aimed at clarifying the range of provisions under the GDPR. Three were adopted in 2019 and finalised in the same year, following a public consultation. Two Guidelines were adopted in 2019 and subsequently submitted to public consultation. These had not yet been finalised by the end of 2019.

The adopted Guidelines addressed codes of conduct and monitoring bodies at a national and European level, as well as clarifying the processing of personal data under a range

of circumstances, namely during the provision of online services, through video devices, on the principles of Data Protection by Design & Default, and related to the Right to be Forgotten by search engines.

Three Guidelines adopted in 2018 were approved by the EDPB in their final form in 2019, following public consultations. These Guidelines clarify accreditation and certification criteria and the territorial scope outlined in the GDPR.

Guidance provides stakeholders with a consistent interpretation of their rights and obligations.

The EDPB also issued a recommendation on the draft list submitted by the European Data Protection Supervisor (EDPS) on processing operations which require a Data Protection Impact Assessment.

5.1.1. Guidelines on Codes of Conduct

During its seventh plenary meeting on 12 February 2019, the EDPB adopted the Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.

The aim of these Guidelines is to provide practical guidance and interpretative assistance in relation to the application of Articles 40 and 41 of the GDPR. They clarify the procedures and rules involved in the submission, approval and publication of codes of conduct at both national and European level.

These Guidelines should provide all competent SAs, the EDPB and the European Commission with a clear framework to evaluate codes of conduct in a consistent manner and to streamline the procedures involved in the assessment process.

A public consultation was launched following the adoption of the document. The final version of the Guidelines, including further points of clarification, was adopted on 4 June 2019.

5.1.2. Guidelines on the processing of personal data in the context of online services

On 9 and 10 April 2019, the EDPB met for its ninth plenary session. During this meeting, the EDPB adopted the Guidelines 2/2019 on the processing of personal data under Article 6.1.b of the GDPR in the context of the provision of online services to data subjects. These Guidelines aim to clarify the scope and application of Article 6.1.b GDPR on lawfulness of processing, in the context of information society services.

The Guidelines make general observations regarding data protection principles and the interaction of Article 6.1.b GDPR with other lawful bases. In addition, they contain guidance on the applicability of Article 6.1.b GDPR in the context of bundling of separate services and termination of contract.

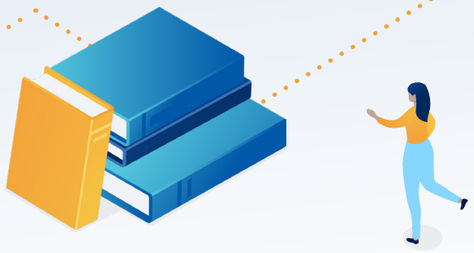
The document was subject to a public consultation. The final version of the Guidelines was adopted on 8 October 2019.

5.1.3. Recommendation on the EDPS draft list on processing operations subject to Data Protection Impact Assessments (DPIAs)

During its twelfth plenary meeting held on 9 and 10 July 2019, the EDPB adopted the Recommendation 1/2019 on the draft list of the EDPS regarding the processing operations subject to the requirement of a Data Protection Impact Assessment.

Article 39.4 of Regulation 2018/1725 requires the EDPS to establish and make public a list of the kind of processing operations which require a DPIA, with the goal of informing data controllers.

The EDPS has to consult with the EDPB prior to adoption of



these lists, since they refer to processing operations by a controller acting jointly with one or more controllers other than EU institutions and bodies.

In its Recommendation, the EDPB invited the EDPS to amend certain wording and examples around sensitive data, large-scale data processing, combined datasets, and vulnerable data subjects.

5.1.4. Guidelines on processing of personal data through video devices

During its July plenary meeting, the EDPB also adopted the Guidelines 3/2019 on processing of personal data through video devices.

The Guidelines clarify how the GDPR applies to the processing of personal data in the context of video surveillance, and cover both traditional video devices and smart video devices. For the latter, the Guidelines focus on the rules regarding the processing of special categories of data.

Other areas covered by the Guidelines include the lawfulness of processing, the applicability of the household exemption, and the disclosure of footage to third parties.

The Guidelines were subject to a public consultation, which closed on 9 September 2019. A final version of the document was adopted by the EDPB in early 2020, taking into account input from the consultation.

5.1.5. Guidelines on Data Protection by Design and by Default

During its fifteenth plenary meeting on 13 November 2019, the EDPB adopted the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

The Guidelines focus on the obligation of Data Protection by Design and by Default as set forth in Article 25 GDPR. This requires that controllers implement appropriate technical and organisational measures, as well as the necessary safeguards, to establish data protection principles and to protect the rights and freedoms of data subjects. Controllers must also be able to demonstrate that the implemented measures are effective.

In 2019, the EDPB adopted Guidelines concerning Codes of Conduct, data processing in the context of online services and through video devices, Data Protection by Design and by Default, and the Right to be Forgotten.

The Guidelines cover elements that controllers must take into account when designing the processing, such as the cost of setting up and maintaining up-to-date technology, in addition to the nature, scope, context, and purpose of the processing itself. The Guidelines also contain practical guidance on how to effectively implement data protection principles, listing key design and default elements as well as illustrating practical cases.

The Guidelines were submitted for public consultation, which remained open until 16 January 2020. A final version of the document will be adopted by the EDPB later in 2020, taking this consultation into account.

5.1.6. Guidelines on the Right to be Forgotten

During its sixteenth plenary meeting on 2 December 2019, the EDPB adopted the first part of the Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR.

The Guidelines provide an interpretation of Article 17 GDPR, which outlines the "Right to request delisting". Following the Costeja vs. Google Spain judgment of the Court of Justice of the European Union (CJEU) of 13 May 2014, which established this right, a data subject may request that a search engine provider erase webpage links redirecting to his or her personal data.

The Guidelines seek to establish the grounds and exceptions for delisting requests made to search engine providers.

To gather feedback on the Guidelines, the EDPB launched a public consultation, open until 5 February 2020.

5.1.7. Guidelines adopted following public consultation

In 2019, the EDPB approved a final version of three Guidelines already adopted in draft form in 2018.

- **Guidelines on Certification and Identifying Certification Criteria**: On 23 January 2019, the EDPB adopted the final version of the core text of Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the GDPR, taking into account the contributions received during a public consultation. The primary aim of these Guidelines is to identify relevant criteria for certification mechanisms, which can be used by organisations to demonstrate compliance with the GDPR.
- On the same day, the **Annex on the Guidelines on Certification and Identifying Certification Criteria** was adopted and submitted for public consultation. The Annex identifies topics that SAs and the EDPB will consider and apply for the approval of certification criteria for a certification mechanism. The entire Guidelines, including a corrigendum and the Annex, were finalised in June 2019.
- **Guidelines on Accreditation and Certification Bodies**: These Guidelines were adopted on 6 February 2018. The core text was finalised on 4 December 2018. On the same day, Annex 1 was adopted. The entire Guidelines, including Annex 1, were adopted in their final form in June 2019.
- **Guidelines on Territorial Scope**: On 12 November 2019, the EDPB adopted the final version of the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), following a public consultation. These Guidelines assess whether a particular data processing operation falls within the territorial scope of the GDPR and clarify the application of the Regulation in various situations, for example, when the data controller or processor is established outside the EEA.

5.2. CONSISTENCY OPINIONS

National SAs from EEA countries must request an Opinion from the EDPB before adopting any decision on subjects specified by the GDPR as having cross-border implications. This applies when a national SA:

- intends to adopt a list of the processing operations subject to the requirement for a Data Protection Impact Assessment (DPIA);
- intends to adopt a draft code of conduct relating to processing activities;
- aims to approve the criteria for accreditation of a certification body;
- aims to adopt standard data protection clauses or contractual clauses;
- aims to approve binding corporate rules.

The competent SA has to take utmost account of the Opinion. In addition, any SA, the Chair of the EDPB or the Commission may request that any matter of general application or which has consequences for more than one Member State be examined by the EDPB with a view to obtaining an Opinion. This can also apply in cases where a competent SA does not comply with obligations for mutual assistance or for joint operations.

The aim of these Opinions is to guarantee the consistent application of the GDPR by national SAs.

5.2.1. Opinions on the draft Data Protection Impact Assessment lists (DPIAs)

In 2019, the EDPB adopted five Opinions on the draft lists submitted by national SAs on processing operations which require a DPIA, namely those submitted by SAs in Liechtenstein, Norway, Spain, Iceland, and Cyprus.

These lists form an important tool for the consistent application of the GDPR across the EEA. DPIA is a process that helps to identify and mitigate data protection risks that may affect the rights and freedoms of individuals.

While in general the data controller must assess if a DPIA is required before engaging in the processing activity, national SAs must establish and list the kind of processing operations for which a DPIA is required.

These Opinions follow the 26 DPIA-related Opinions adopted by the EDPB in 2018, and will further contribute to establishing common criteria for assessing where DPIAs are required.

In addition, the EDPB also issued three Opinions on the draft lists submitted by SAs in the Czech Republic, Spain and France on the processing operations exempt from a DPIA. Contrary to the "black lists", the adoption of "white lists" of DPIAs are not mandatory for EEA SAs.

5.2.2. Opinion on transfers of personal data between EEA and non-EEA Financial Supervisory Authorities

During its seventh plenary meeting on 12 February 2019, the EDPB adopted Opinion 4/2019 on the draft Administrative Arrangement for the transfer of personal data between European Economic Area (EEA) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities.

The Administrative Arrangement is based on Article 46.3.b GDPR and outlines rules and commitments for transfers of personal data between EEA Financial Supervisory Authorities, including the European Securities and Markets Authority (ESMA), and their non-EEA counterparts.

Following the Opinion, this arrangement will be submitted to the competent SAs for authorisation at national level. The EDPB recommends that the SAs monitor the arrangement and its practical application to ensure that data subject rights and appropriate means of redress and supervision are effective and enforceable in practice.

5.2.3. Opinion on the interplay between the ePrivacy Directive and the GDPR

During its eighth plenary meeting on 13 and 14 March 2019, the EDPB adopted Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.

The Opinion seeks to clarify whether the processing of personal data falls under the scope of both the GDPR and the ePrivacy Directive, and whether this limits the competences, tasks and powers of data protection authorities under the GDPR.

The EDPB is of the opinion that SAs are competent to enforce the GDPR. The fact that a subset of the processing falls within the scope of the ePrivacy Directive does not limit the competence of SAs under the GDPR.

Indeed, an infringement of the GDPR may at the same time constitute an infringement of national ePrivacy rules. SAs may take this into consideration when applying the GDPR (e.g. when assessing compliance with the lawfulness or fairness principles).

5.2.4. Opinion on the competence of a Supervisory Authority in case of a change in circumstances relating to the main or single establishment

During its twelfth plenary meeting on 9 and 10 July 2019, the EDPB adopted Opinion 8/2019 on the competence of a Supervisory Authority in case of a change in circumstances relating to the main or single establishment.

The scenario outlined in the Opinion may occur when the main establishment is relocated within the EEA, or is moved to the EEA from a third country, or when there no longer is a main or single establishment in the EEA. In such circumstances, the EDPB is of the opinion that the competence of the Lead Supervisory Authority (LSA) can switch to another SA.

In this case, the cooperation procedure set forth under Article 60 GDPR will continue to apply and the new LSA will be obligated to cooperate with the former LSA, as well as the other concerned SAs (CSAs), to reach a consensus. The switch can take place as long as no final decision has been reached by the competent SA.

5.2.5. Opinions on Accreditation Criteria for monitoring bodies of Codes of Conduct

During its July plenary meeting, the EDPB also adopted Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to Article 41 GDPR. The EDPB agreed that all codes covering non-public authorities and bodies are required to have accredited monitoring bodies in accordance with the GDPR.

In addition, during its sixteenth plenary meeting on 2 and 3 December 2019, the EDPB adopted Opinion 17/2019 on the UK data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to Article 41 GDPR. In this Opinion, the EDPB proposed some changes to the draft accreditation requirements in order to ensure consistent application of the accreditation of monitoring bodies.

5.2.6. Opinion on Standard Contractual Clauses for processors by Danish SA

In July, the EDPB adopted Opinion 14/2019 on the draft Standard Contractual Clauses (SCCs) submitted by the DK SA (Article 28.8 GDPR). As the first Opinion on this topic, it aims to ensure the consistent application of Article 28.8 GDPR for contracts between controller and processor.

Standard Contractual Clauses (SCCs) aim to help organisations meet the requirements of Article 28.3 and 28.4 GDPR, given that the contract between controller and processor cannot simply restate the provisions of the GDPR but should further specify them, e.g. with regard to the assistance provided by the processor to the controller.

National SAs from EEA countries must request an Opinion from the EDPB before adopting any decision on subjects specified by the GDPR as having cross-border implications.

The EDPB made several recommendations which were taken into account by the Danish SA, which subsequently updated the draft SCCs.

The possibility of using SCCs adopted by an SA does not prevent the parties from adding other clauses or additional safeguards, provided that they do not , directly or indirectly contradict the adopted clauses or prejudice data subjects' fundamental rights or freedoms.

Nevertheless, the clauses are an instrument to be used 'as is', i.e. the parties who enter into a contract with a modified version of the clauses are not considered to have used the adopted SCCs.

5.2.7. Opinions on Binding Corporate Rules

During its fourteenth plenary meeting on 8 and 9 October 2019, the EDPB adopted Opinion 15/2019 on the draft decision of the competent Supervisory Authority of the United Kingdom regarding the Binding Corporate Rules (BCRs) of Equinix Inc, following a request by the UK Information Commissioner's Office (ICO).

The EDPB is of the opinion that the Equinix BCRs contain all elements required under Article 47 GDPR and WP 256 rev01, and contain the appropriate safeguards.

In case of Brexit, the company committed to initiate a new process of approval with an alternative SA as new Lead BCR SA without undue delay and, in the event, within one calendar month.

During its November plenary meeting, the EDPB adopted Opinion 16/2019 on the draft decision of the Belgian Supervisory Authority regarding the Binding Corporate Rules of ExxonMobil Corporation.

The EDPB is of the opinion that the draft controller BCRs provide sufficient safeguards in line with Article 46.2.b GDPR and comply with Article 47 GDPR.

5.3. LEGISLATIVE CONSULTATION

The EDPB advises the European Commission on any issue related to the protection of personal data, on the format and procedures for information exchange between companies and SAs under Binding Corporate Rules (BCRs), and on certification requirements. The EDPB also advises the European Commission when assessing the adequacy of the level of data protection in third countries or international organisations.

In 2019, the EDPB issued an Opinion on the interplay between the Clinical Trials Regulation (CTR) and the GDPR, requested by the European Commission's Directorate-General for Health and Food Safety (DG SANTE).

The EDPB is also subject to Article 42 of Regulation 2018/1725 on legislative consultation. This allows the EDPS and the EDPB to coordinate their work with a view to issuing a Joint Opinion.

In 2019, the EDPB and the EDPS adopted a Joint Opinion concerning the data protection aspects of the eHealth Digital Service Infrastructure. This Opinion was also issued following DG SANTE's request.

The EDPB also adopted, on its own initiative, a statement on the draft ePrivacy Regulation and issued a contribution on the data protection aspects of the Budapest Convention on Cybercrime.

5.3.1. EU-U.S. Privacy Shield

Representatives of the EDPB participated in joint reviews of the EU-U.S. Privacy Shield adequacy decision, conducted by the European Commission to assess its robustness and practical implementation. The EDPB issued reports on the Second and Third Annual Review of the EU-U.S. Privacy Shield.

During its January plenary meeting, the EDPB adopted its report on the Second Annual Joint Review of the EU-U.S. Privacy Shield, which was conducted by the European Commission in October 2018 with the support of the EDPB's representatives.

The EDPB welcomed efforts made by the United States authorities and the European Commission to implement the EU-U.S. Privacy Shield, such as adapting the initial certification process, starting ex-officio oversight and expanded enforcement. These actions also included enhanced transparency, following the decision to publish a

number of important documents, in part via declassification by the United States Foreign Intelligence Surveillance Court.

The EDPB also welcomed the appointment of a new Chair and three new members of the Privacy and Civil Liberties Oversight Board (PCLOB), and a permanent Ombudsperson.

However, the EDPB had a number of significant concerns – already expressed by the EDPB's predecessor, the Article 29 Working Party (WP29) – about the lack of concrete assurances aimed at excluding indiscriminate collection and access of personal data for national security purposes.

In addition, the EDPB did not consider the Ombudsperson to have been vested with sufficient powers to remedy non-compliance. The EDPB also pointed out that checks regarding compliance with the substance of the EU-U.S. Privacy Shield's principles were not sufficiently strong.

The EDPB had some additional concerns about the checks needed to comply with the onward transfer requirements, the scope of the meaning of HR Data, and the recertification process, as well as several issues still pending after the first joint review.

During its November plenary meeting, the EDPB adopted its Third Annual Joint Review report on the EU-U.S. Privacy Shield. In its report, the Board welcomed the appointments of the last missing members of the PCLOB and noted that several issues previously raised remained unsolved. More generally, the EDPB found that the Review Team members would benefit from broader access to non-public information concerning commercial aspects and ongoing investigations.

Regarding the collection of data by public authorities, the EDPB encourages the PCLOB to issue and publish further reports in order to provide an independent assessment of surveillance programmes conducted outside U.S. territory, when data is transferred from the EU to the U.S. The EDPB reiterated that its security-cleared experts remain ready to review further documents and discuss additional classified elements.

While the EDPB welcomed the new elements provided during the 2019 review process, it still could not conclude that the Ombudsperson is vested with sufficient powers to access information and remedy non-compliance.

5.3.2. Opinion on clinical trials Q&A

Under Article 70 GDPR, the European Commission can submit a request for consultation to the EDPB. In 2018, the Commission's DG SANTE requested a consultation on a document on "Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)".

The EDPB subsequently adopted Opinion 3/2019 during its January plenary meeting. The Opinion addressed in particular the adequate legal bases of personal data processing in the context of clinical trials and the secondary uses of clinical trial data for scientific purposes.

5.3.3. Statement on the future ePrivacy Regulation

During its eighth plenary meeting in March 2019, the EDPB adopted Statement 3/2019 on an ePrivacy regulation.

The EDPB called upon EU legislators to intensify efforts towards the adoption of the ePrivacy Regulation, which is essential to complete the EU's data protection framework and the confidentiality of electronic communications.

The future ePrivacy Regulation should under no circumstance lower the level of protection offered by the current ePrivacy Directive and should complement the GDPR by providing additional guarantees for all types of electronic communications.

5.3.4. Additional protocol to the Budapest Convention on Cybercrime

In November 2019, the EDPB adopted a contribution to the draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), to be considered within the framework of consultations held by the Council of Europe Cybercrime Convention Committee (T-CY).

The EDPB highlighted that the protection of personal data and legal certainty must be guaranteed, thus contributing to establishing sustainable arrangements for the sharing of personal data with third countries for law enforcement

purposes, which are fully compatible with the EU Treaties and the Charter of Fundamental Rights.

5.3.5. EDPB-EDPS Joint Opinion on the eHealth Digital Service Infrastructure

During its July 2019 plenary meeting, the EDPB and the EDPS adopted Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI).

This was the first Joint Opinion by the EDPB and the EDPS. It was adopted in response to a request from the European Commission under Article 42.2 of Regulation 2018/1725 on data protection for EU institutions and bodies.

The eHealth Network is a voluntary network of authorities responsible for eHealth, as designated by Member States. One of its main objectives is to enhance interoperability between national digital health systems, by exchanging patient data contained in ePrescriptions, Patient Summaries and electronic health records. In this framework, the eHealth Network and the Commission have developed an IT tool, the eHealth Digital Service Infrastructure (eHDSI).

In their Opinion, the EDPB and EDPS considered that, in this specific situation and for the concrete processing of patients' data within the eHDSI, there was no reason to dissent from the European Commission's assessment of its role as a processor within the eHDSI. Furthermore, the Joint Opinion stressed the need to ensure that all processing duties of the Commission in this operation were clearly set out in the relevant Implementing Act, as specified in the applicable data protection legislation.

5.4. OTHER DOCUMENTS

5.4.1. Information note on data transfers under the GDPR in the event of a no-deal Brexit

During its February 2019 plenary, the EDPB adopted an information note on data transfers under the GDPR in the event of a no-deal Brexit, addressed to commercial entities and public authorities.

With regards to the transfer of personal data **from the EEA to the UK**, the EDPB recommended basing the process on one of the following instruments:

- Standard or ad hoc Data Protection Clauses;
- Binding Corporate Rules;
- Codes of Conduct and Certification Mechanisms;
- Specific instruments available to public authorities.

In the absence of Standard Data Protection Clauses or other alternative appropriate safeguards, derogations can be used under certain conditions, as outlined by Article 49 GDPR.

5.4.2. Information note on Binding Corporate Rules for companies which have the UK Information Commissioner's Office as BCR Lead Supervisory Authority

In February 2019, the EDPB also issued an information note to companies having the UK Information Commissioner's Office (ICO) as their BCR LSA in the event of a no-deal Brexit.

5.4.3. Statement on the US Foreign Account Tax Compliance Act

On 25 February 2019, the EDPB adopted Statement 01/2019 on the US Foreign Account Tax Compliance Act (FATCA), following the European Parliament's resolution on the adverse effects of the FATCA on EU citizens.

European SAs have long been aware of the data protection issues raised by the automatic exchange of personal data for tax purposes. In its statement, the EDPB referred to previous work on the FATCA by its predecessor, the Article 29 Working Party (WP29).

The EDPB also acknowledged the Parliament's call to review existing data protection safeguards authorising the transfer of personal data to the United States' Internal Revenue Service (IRS) for the purposes of the FATCA. In this regard, the EDPB has already initiated work on Guidelines on the elaboration of transfer tools based on Articles 46.2.a and 46.3.b GDPR.

These Guidelines will include information on minimum guarantees to be included in legally binding and enforceable instruments concluded between public authorities and bodies, as well as data protection provisions to be included in administrative arrangements between public authorities or bodies.

It should be noted that legally binding instruments do not require specific authorisation from an SA, whereas any provisions to be included in administrative arrangements are subject to such authorisation.

This set of Guidelines, to be adopted in 2020, will also be a useful tool for evaluating the compliance of intergovernmental agreements signed between Member States and the United States government on FATCA with the GDPR.

5.4.4. Statement on the use of personal data in political campaigns

During its March 2019 plenary meeting, the EDPB adopted Statement 2/2019 on the use of personal data in the course of political campaigns, in light of the 2019 European Parliament elections and other elections taking place across the EU and beyond.

Data processing techniques for political purposes can pose serious risks to privacy and data protection rights, as well as to the integrity of the democratic process. In its statement, the EDPB highlighted a number of key points to be taken into consideration when political parties process personal data during their electoral activities.

1. Under the GDPR, personal data revealing political opinions is a special category of data and its processing is heavily limited, if not entirely prohibited.
2. Personal data made public, for example on social media, is still subject to EU data protection law.
3. Even where data processing is lawful, organisations must respect their duties of fairness and transparency to individuals whose data has been collected. Political parties and candidates must stand ready to demonstrate how they have complied with data protection principles.
4. Automated decision-making, including profiling, is only lawful with the valid explicit consent of the data subject.
5. In case of targeting, adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it, and how they can exercise their rights as data subjects. In addition, certain Member States require transparency in matters of paid political advertisements.

The EDPB's statement reiterated the importance of compliance with data protection rules to protect democracy, preserve citizens' trust and confidence, and safeguard the integrity of elections. The EDPB encourages maximum cooperation among SAs in monitoring and enforcing these rules.

5.4.5. LIBE Report on the implementation of the GDPR

On 26 February 2019, the EDPB LIBE report on the implementation of GDPR was issued following a request made by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs Committee (LIBE).

This document provides an overview of the implementation and enforcement of the GDPR covering both the cooperation mechanism and the consistency findings.

Nine months after the GDPR's entry into application, the EDPB concluded that the GDPR cooperation and consistency mechanism works quite well in practice. National SAs make daily efforts to facilitate this cooperation, via written and oral communication.

However, these cooperation duties do entail additional workload and time resources, which in turn can have an impact on SAs' budgets. The handling of cross-border cases in particular takes a considerable amount of time, given the need for thorough investigations and compliance with national procedural rules. The EDPB noted that national SAs must tackle challenges regarding the harmonized enforcement of the GDPR.

Finally, while the EDPB reported six final One-Stop-Shop (OSS) cases, it could not provide testimony about the effectiveness of the consistency mechanism for these, since no dispute resolution was necessary during the reporting period.

5.4.6. EDPB pleading before the CJEU in Case C-311/18 (Facebook Ireland and Schrems)

On 9 July 2019, the EDPB Chair appeared before the Court of Justice of the European Union (CJEU), which requested an oral pleading on Case C-311/18 (Facebook Ireland and Schrems).

The case arose from a preliminary reference made by the Irish High Court to the CJEU, following a legal challenge brought by Austrian privacy activist Max Schrems in relation to Facebook's use of Standard Contractual Clauses (SCCs) to transfer data from Facebook Ireland to servers located in the United States. Mr. Schrems argued that Facebook Inc.'s obligation to make the personal data of its users available to the United States authorities in charge of surveillance programmes threatened the exercise of the rights guaranteed in Article 7, 8 and 47 of the Charter, and that no remedies were put in place. In this context, the CJEU invited the EDPB to participate in the oral hearing that took place on 9 July 2019.

In its pleading, the EDPB answered several questions asked by the CJEU. The EDPB underlined the difference between SCCs and adequacy decisions and stated that, with regard to the SCCs, the European Commission is not obliged to examine the continuity of the protection afforded by EU law. In this regard, the EDPB considered that verifying the compliance of transfers with the EU data protection law when considering whether to enter into the SCCs should be primarily the responsibility of the exporter and the importer. This should be further assessed by the competent SA, which may suspend transfers if it finds that exporter and importer did not comply with their obligations under the SCCs.

The EDPB's view was that the continuity of data protection afforded under EU laws also needs to be ensured during data transit to a third country, no matter which transfer tool is used. This includes data outside or on its way to the EU's physical borders.

With regard to questions on adequacy decisions, the EDPB stated that all domestic rules are relevant for the assessment of adequacy and that data subjects should be able to enforce their rights before the third country's courts. In this regard, even though the establishment of the Ombudsperson mechanism under the Privacy Shield framework is welcomed, the EDPB stressed that it cannot conclude that the Ombudsperson constitutes an effective remedy before a tribunal in the meaning of Article 47 of the Charter of Fundamental Rights.

Finally, the EDPB stressed the importance of the role of the SAs in upholding and spreading EU standards on the fundamental right to data protection.

At the time of this report going to press, the CJEU had not yet issued a final ruling on the case.

5.5. PLENARY MEETINGS AND SUBGROUPS

Between 1 January and 31 December 2019, the EDPB held 11 plenary meetings. The agendas of the plenary sessions are published on the EDPB website. During these meetings, the EDPB adopted Guidelines, Opinions, and other documents such as statements or informative notes to advise the European Commission, national Supervisory Authorities, and other stakeholders on GDPR matters, as outlined earlier in this chapter.

In addition, there were 90 expert subgroup meetings. The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks. The list of the expert subgroups and their respective mandates are available in Section 9.

5.6. STAKEHOLDER CONSULTATIONS AND TRANSPARENCY

5.6.1. Stakeholder events on future guidance

The EDPB organises stakeholder events to gather input and views on issues in the interest of developing future guidance. In 2019, the EDPB organised three such events focusing on the revised Payments Services Directive (PSD2), on the concepts and responsibilities of controllers and processors, and on data subject rights.

5.6.1.1. Interplay of PSD2 and GDPR

On 27 February 2019, the EDPB's Financial Matters Expert Subgroup (FMES) organised a workshop on the revised Payments Services Directive (PSD2), in order to collect stakeholders' views and inform future Guidelines.

> The EDPB organises stakeholder events to gather input and views on issues in the interest of developing future guidance.

Of the event's 39 participants, 16 were external stakeholders. Representatives from banking federations, payment institutions federations, consumer protection associations, academia, and the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) presented at the workshop. Other participants included collection associations, credit information suppliers, banks, and financial market associations.

The discussions highlighted the key areas already identified by the FMES where guidance is required, as well as providing concrete examples. The feedback will be used as basis for developing Guidelines on PSD2.

5.6.1.2. Concepts of controller and processor

On 25 March 2019, the EDPB organised a full-day stakeholder event to gather the views of EU sector organisations and NGOs in the context of the EDPB's recast of the Article 29 Working Party's Opinion 1/2010 on the concepts of controller and processor. Around 80 participants, including EDPB representatives, attended the event, which received positive feedback overall.

To facilitate greater engagement, core discussions took place in three smaller breakout sessions with rotating rapporteurs and moderators. Each group addressed the following topics:

- **The concepts of controller and processor**: issues raised related to the relationship between controllers and processors, the main criteria for identifying the controller, clarification of other concepts such as

recipient and third party, and the consistent application of the Guidelines. Additionally, stakeholders suggested including as many practical examples as possible.

- **The specific obligations of processors and the contracts between controllers and processors**: stakeholders highlighted the need to revise the current guidance to reflect changes in the legal framework and the business environment, and voiced concern over the difficulty to implement certain new duties for processors, especially SMEs. Stakeholders also identified a need for guidance on the controller's audit rights, the obligation for the processor to inform the controller in case of an infringement, and duties regarding sub-processors.
- **Joint controllership**: stakeholders once more stressed the changed business context for data sharing and highlighted difficulties when incorporating practical duties in contracts. They suggested that guidance should further clarify the criteria to be taken into account when determining whether the relationship qualifies as joint controllership.

The feedback provided by stakeholders and especially the need for practical examples will be considered when drafting the guidelines.

5.6.1.3. Data subject rights

On 4 November 2019, the EDPB organised a full-day stakeholder event on the topic of data subject rights. Attendees included representatives from individual companies, sector organisations, NGOs, law firms, and academia.

Developing guidance on data subject rights is one of the EDPB's 2020 priorities. During the event, around 160 participants, including EDPB representatives, had the opportunity to share their experiences on this topic and raise issues.

The workshop followed a similar format as the March 2019 event, which proved to be engaging for stakeholders. Discussions were spread across three smaller breakout sessions with rotating rapporteurs and moderators, each addressing the following topics:

- **Right of access**: issues raised related to the type and format of information requested, formal requirements such as identity verification and dedicated channels, and clarifications on third-party access requests.
- **Right to rectification and right to erasure**: stakeholders shared concerns on differences and interplays between rights, technical means and proof of erasure, and requests involving joint controllers or controllers outside the EEA.
- **Right to restrict processing and right to object**: stakeholders asked for concrete examples, as well as guidance on the practical implementation of restriction and issues of legitimate interest, especially related to direct marketing.

The EDPB will take into account input provided during the workshop, including the practical examples shared by the stakeholders, the guidance requested and the questions raised. In 2020, the relevant expert subgroup will further discuss the topics and work on Guidelines.

5.6.2. Public consultations on draft guidance

Following the preliminary adoption of Guidelines, the EDPB organises public consultations to give stakeholders and citizens the opportunity to provide additional input. This input is then taken into account by the EDPB members in charge of drafting. Next, the Guidelines are adopted in their final version.

To further enhance transparency, the EDPB adapted its website to enable the publication of stakeholders' contributions to public consultations.

In 2019, the EDPB launched five such consultations:

- In February, the EDPB opened two public consultations, on Guidelines on Codes of Conduct (1/2019) and on the Annex to the Guidelines on Certification (1/2018), for which it received 44 and 8 contributions respectively. The final versions of the Guidelines and of the Annex, including further points of clarification, were adopted in June.
- In April, the EDPB opened a public consultation on Guidelines on the processing of personal data in the context of online services (2/2019), receiving 45 contributions.
- In July, the EDPB opened a public consultation on Guidelines on video surveillance (3/2019), receiving 94 contributions.
- In November, the EDPB opened a public consultation on Guidelines on Data Protection by Design and by Default (4/2019). This consultation was still open at the end of 2019.
- In December, the EDPB opened a public consultation on Guidelines on the Right to be Forgotten in the search engine cases (5/2019). This consultation was still open at the end of 2019.

5.6.3. Stakeholder survey on adopted guidance

For the second year in a row, the EDPB conducted a survey as part of the annual review of the Board's activities under Article 71.2 GDPR. Questions focused on the content and adoption process of the EDPB's Guidelines, with a view to understanding to what extent stakeholders find them helpful and practical to interpret GDPR's provisions.

5.6.3.1. Participants

53 entities including organisations and individual companies, representing different countries, sectors and business sizes participated in the survey. The majority of respondents were based in Europe (50 organisations), while the remaining three were based in North America.

The financial, banking and insurance sector was the most represented, with 17 contributors, followed by wholesale and retail trade (nine respondents), information technologies (six respondents), human health and social work activities (six respondents), and human and fundamental rights (three respondents).

More than 60 percent of respondents were representing small entities, with less than 250 employees.

The results showed that participants had consulted, on average, four Guidelines.

5.6.3.2. Findings

In line with the results of the 2018 survey, 64 percent of stakeholders participating in the survey found the Guidelines to be useful and 46 percent considered them to be sufficiently pragmatic and operational for their needs. One of the suggestions was to avoid long pages of guidelines and to include checklists to better guide the companies.

In addition, 62 percent of those who responded to the survey found the Guidelines easy to read. There was a marked increase of respondents who found the guidelines easily accessible on the EDPB's website: nearly 80 percent, up from 64 percent in 2018.

On the first section of the survey, dedicated to the Guidelines' content, the majority of respondents welcomed the pan-European applicability of the Guidelines, judging that this prevents national fragmentation. Half of the respondents judged the Guidelines to provide sufficient examples in their respective area of regulation, and one of the respondents expressed appreciation for the fact that the EDPB guidelines include many real-life examples.

Stakeholders encouraged further interpretative work but noted that the Guidelines are a useful tool in supporting the application of the GDPR.

Further interpretative work was encouraged to clarify, for example, the relationship between controller and processor and the legal basis of legitimate interest. The EDPB welcomes this timely feedback as it schedules an update of the dedicated Article 29 Working Party Guidelines, to be carried out during 2020, in line with the 2019-2020 EDPB Work programme.

Compliance with the GDPR for SMEs remains a challenge, but stakeholders noted that the EDPB's Guidelines are a useful tool in supporting its application.

40 percent of stakeholders found the consultative process appropriate to satisfying. They welcomed the EDPB's openness to public consultations and the opportunities given to express views on the Board's work. Part of the respondents appreciated the clarity and accessibility of the EDPB's workshops, but encouraged further improvements in transparency.

5.6.3.3. Conclusions

The EDPB highly appreciated the stakeholders' participation and was pleased to see that respondents acknowledged the Guidelines' usefulness. Feedback on the Guidelines' operational value and alignment with other EU laws was equally appreciated, as it gave precious insights into stakeholder needs, and will inform the Board's work moving forward.

The EDPB also welcomed stakeholders' value of transparency and interest in participating in the adoption process. In 2020, the EDPB is committed to continuing its cooperation and outreach to inform the development and effectiveness of future guidance.

5.6.4. Transparency and access to documents

Transparency is a core principle of the EDPB and in 2020, the EDPB will continue to implement measures designed to increase the transparency of its work. As an EU body, the EDPB is subject to Article 15 of the Treaty of the Functioning of the European Union and Regulation 1049/2001 on public access to documents. Article 76.2 GDPR and Article 32 of the EDPB's Rules of Procedure (RoP) reinforce this requirement.

Upholding the principle of transparency means that any citizen of the European Union and any natural or legal person residing or having its registered office in a Member State has the right to access EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities.

In exceptional cases, the EDPB can refuse to disclose a document, or part of it. The reasons for refusal and other procedural rules are outlined in the EU Public Access Regulation.

In 2019, the number of public access requests registered for documents held by the EDPB was 39.

5.7. EXTERNAL REPRESENTATION OF THE BOARD

Public awareness and cooperation are vital to upholding data protection rights in the EEA and beyond, which is why the EDPB values stakeholder and citizen engagement.

The EDPB Secretariat supports the Chair and the Deputy Chairs in engagements with other EU institutions or bodies and when they represent the EDPB at conferences and multi-stakeholder platforms.

Staff members from the EDPB Secretariat also take part in several events to present the activities of the EDPB.

5.7.1. Participation of Chair and Deputy Chair in conferences and speaking engagements

5.7.1.1. Chair of the EDPB

In 2019, EDPB Chair Andrea Jelinek had 34 speaking engagements, including keynote speeches, presentations and panel debates in a range of institutes, think tanks and forums. She also met with EU Commissioners and travelled to meet with data protection officials from countries outside the EEA.

During the G20 meeting in Tokyo, Japan, the Chair took part in a side event entitled "**DPAs' role in Global Data Flows**", held on 3 July 2019 and organised by the Japanese Data Protection Authority.

In her opening remarks, the Chair explained the role of the EDPB, its activities so far and the importance of international convergence. She also talked about the EU-Japan adequacy decision, stressing its importance as a model for successful international cooperation.

On 9 July, the Chair was invited to a **hearing at the Court of Justice of the European Union** (CJEU) in Luxembourg, concerning Case C-311/18 (Facebook Ireland and Schrems).

The Chair of the EDPB also met twice with the **European Parliament's Committee on Civil Liberties, Justice and Home Affairs Committee** (LIBE Committee), in February and in December. These meetings provided the opportunity to present the EDPB's work and to give an overview of GDPR's implementation.

In 2019, the EDPB became Observer of the **International Conference of Data Protection and Privacy Commissioners** (ICDPPC, now the Global Privacy Assembly – GPA). During the October annual meeting held in Tirana, Albania, the Chair presented the EDPB's work and outlined the GDPR's main provisions, including the cooperation and consistency mechanism.

The Chair of the EDPB also participated in other high-level forums on data protection, such as the **Europe Data Protection Congress** and the **Global Summit of the International Association of Privacy Professionals** (IAPP).

5.7.1.2. Deputy Chair of the EDPB

EDPB Deputy Chair Ventsislav Karadjov took part in six speaking engagements during 2019, mainly in the EU but also in the United States, on the occasion of the third annual review of the EU-U.S. Privacy Shield.

As well as taking part in events organised by the European Commission and the European Union Agency for Cybersecurity (ENISA), the Deputy Chair attended high-level platforms such as the Mobile World Congress (MWC) ministerial meeting, where he spoke about GDPR, data privacy and blockchain.

5.7.2. Participation of the EDPB Members in conferences and speaking engagements

In 2019, EDPB Members represented the EDPB in a number of events. Some of these were organised by trade, consumer, or professional associations dealing with aspects of data protection and the implementation of the GDPR, while other invitations came from academia and think tanks.

Several engagements were organised on the initiative of EU institutions and bodies, such as the European Central Bank, the European Ombudsman, and the European Parliament's LIBE Committee.

EDPB representatives also participated in high-level forums on data protection, such as the ICDPPC and the IAPP Europe Data Protection Congress and Global Summit.

5.7.3. Participation of the EDPB Secretariat Staff in conferences and speaking engagements

In 2019, EDPB Secretariat staff members participated in 35 conferences or other engagements with an average of three per month. They were usually invited to deliver speeches or presentations or to join panel discussions.

5.7.4. Election of representative and substitute to the Stakeholders Cybersecurity Certification Group

During its December 2019 plenary meeting, the EDPB confirmed the appointments of the representative and substitute to the Stakeholders Cybersecurity Certification Group.

The Group was established by the Cybersecurity Act, which entered into force on 27 June 2019. Among its provisions, the Act seeks to establish an EU-wide cybersecurity certification framework. The Group's goal is to provide appropriate governance at the EU level and to support ENISA and the European Commission in facilitating consultation with relevant stakeholders.

The Cybersecurity Act identifies EU SAs as such stakeholders. For this reason, the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CNECT) sent a letter to the EDPB on 1 October 2019, requesting that a representative and a substitute for the Group be appointed.

The Compliance, eGovernment and Health Expert Subgroup (CEH ESG), which has a mandate to deal with certification and accreditation topics, evaluated candidates who volunteered to act as EDPB representatives to the Group. During its meeting of 15 November 2019, the CEH ESG nominated Mr. Desmond de Haan, from the Netherlands, as representative and Ms. Georgia Panagopoulou, from Greece, as substitute. They were subsequently approved and appointed by the EDPB.

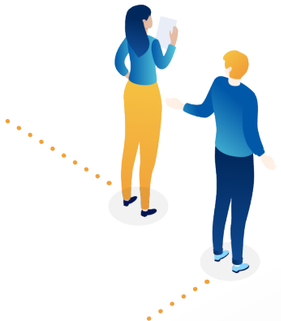
EDPB Annual Report 2019

6

Supervisory Authority activities in 2019

Under the GDPR, Supervisory Authorities (SAs) have a duty to cooperate in order to ensure consistent application of the Regulation. In cases that have a cross-border component, the SAs of the European Economic Area (EEA), i.e. the 28 EU Member States (27 as of 31 January 2020) plus Iceland, Norway and Liechtenstein, have a range of tools at their disposal to facilitate harmonisation. These are:

- mutual assistance;
- joint operation;
- the One-Stop-Shop cooperation mechanism.



6.1. CROSS-BORDER COOPERATION

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

Before starting a One-Stop-Shop procedure for a cross-border case, it is necessary to identify the Supervisory Authority that will lead the investigation (LSA) and the other Concerned Supervisory Authorities (CSAs). The LSA will lead the investigation and draft the decision, while the CSAs will have the opportunity to raise objections.

The LSA is identified as the authority of the EEA country where the data controller or processor under investigation has its main establishment. For example, the place of central administration is one of the criteria used to identify a controller or processor's main establishment.

Further information on this subject is available in Article 1.2 of the Article 29 Working Party Guidelines for identifying a controller or processor's lead Supervisory Authority, endorsed by the EDPB at its first plenary meeting on 25 May 2018.

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

In case of conflicting views regarding which authority should act as LSA, the EDPB will act as a dispute resolution body and issue a binding decision.

Since 25 May 2018, 807 procedures were initiated to identify the LSA and the CSA in cross-border cases. No disputes on the selection of the LSA occurred.

6.1.2. Database regarding cases with a cross-border component

A case with a cross-border component may occur in several situations: when the controller or the processor has an establishment in more than one Member State; when the data processing activity substantially affects individuals in more than one Member State; or when SAs are simply exchanging information, i.e. providing each other with mutual assistance.

Such cases are registered in a central database via the IMI sysem, from which the aforementioned procedures can be initiated.

Since the entry into application of the GDPR, there were 807 cross-border cooperation procedures in the IMI system, out of which 585 cases were started in 2019. Of these cross-border cooperation procedures, 425 resulted from a complaint, while the others originated from other sources, such as investigations, legal obligations or media reports.

6.1.3. One-Stop-Shop Mechanism

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

The LSA must first investigate the case while taking into account national procedural rules, ensuring that the affected individuals are able to exercise their right to be heard, for example. During this phase, the LSA can gather information from another SA via mutual assistance or by conducting a joint investigation.

The IMI system also gives the LSA the opportunity to informally communicate with all CSAs to collect relevant information.

Once the LSA has completed its investigation, it prepares a draft decision, which it then communicates to the CSAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, triggers the EDPB's dispute resolution mechanism.

In such cases, the EDPB will act as a dispute resolution body and issue a binding decision. The LSA must adopt its final decision on the basis of the EDPB's decision.

If the CSAs do not object to either the initial draft or the revised decision, they are deemed to agree with the draft decision.

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

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

By the end of 2019, 142 OSS procedures were initiated by SAs, 79 of which resulted in a final decision.

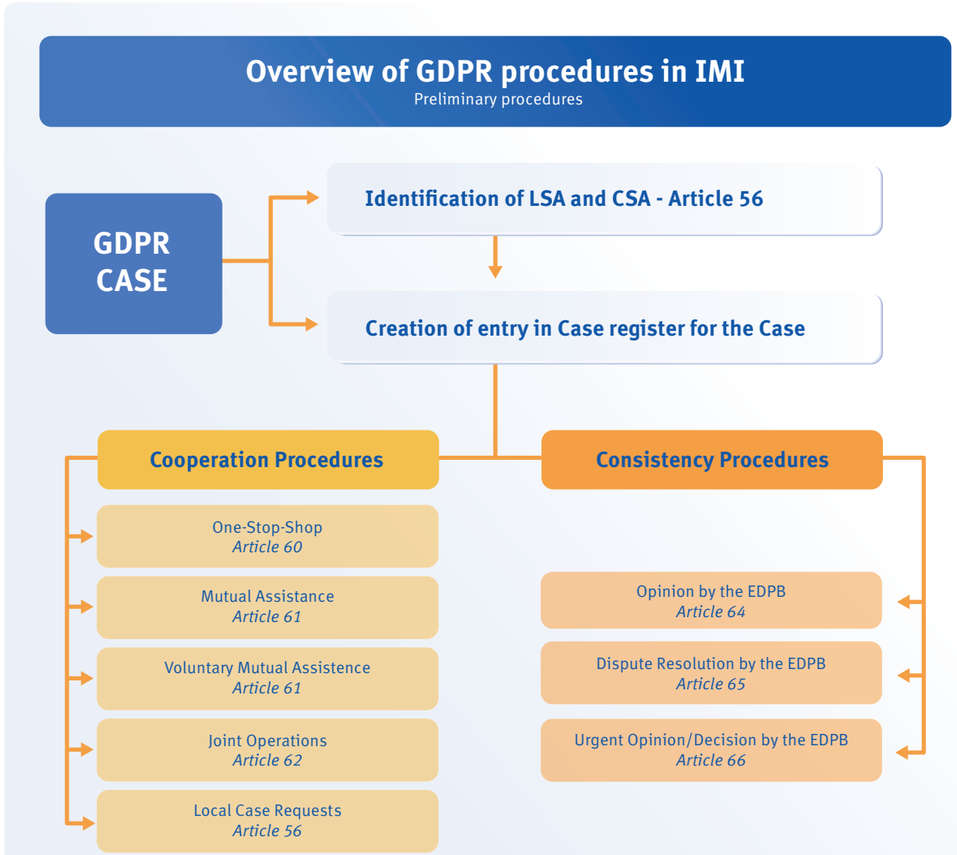
6.1.4. Mutual assistance

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

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

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

Since 25 May 2018, 2,542 mutual assistance procedures were triggered. Of these procedures, the overwhelming majority (2,427) were informal consultation procedures, while 115 were formal requests.



6.1.5. Joint operations

The GDPR allows SAs to carry out joint investigations and joint enforcement measures. Similarly to the mutual assistance procedure, joint operations can be used in the context of cross-border cases subject to the OSS procedure or for national cases with a cross-border component.

In 2019, no joint operations were carried out by SAs.

6.2. NATIONAL CASES[1]

National SAs have different corrective measures at their disposal:

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

6.2.1. Some relevant national cases with exercise of corrective powers

The violations included failure to implement provisions such as privacy by default and design, right to access or right to erasure. Many cases highlighted a lack of proper technical and organisational measures for ensuring data protection, which led to data breaches.

Several significant incidents involved the processing of special categories of data, such as political opinions, credit information or biometric data. The entities fined were from both the private and the public sector.

6.2.1.1. Austria

In 2019, the Austrian SA imposed an administrative fine of EUR 18 million on the Austrian postal service (Österreichische Post AG), ruling that it had violated several provisions of the GDPR. The violations included processing of special categories of data such as political opinions without explicit consent from data subjects. The Austrian SA found an additional violation related to the processing of package and relocation data for direct marketing purposes.

On 12 February, the Austrian SA imposed an immediate ban on these processing operations and ordered the erasure of the data. This decision was followed by the issuing of the administrative fine on 23 October. In both cases, the decisions have been challenged before the Federal Administrative Court.

On 12 August, the Austrian SA imposed an administrative fine of EUR 55,000 on a controller operating in the medical sector. For more than six months, the controller had neither appointed a data protection officer nor had it carried out a DPIA. In addition, the controller had obliged data subjects to give their consent to non-GDPR compliant data processing and had failed to provide them with information required by Articles 13 and 14 GDPR.

6.2.1.2. Belgium

On 28 May 2019, the Belgian SA imposed its first financial penalty since the GDPR entered into force. The administrative fine amounted to EUR 2,000 and concerned the misuse of personal data for election purposes. In taking this decision, the SA stressed that matters of data protection should be considered especially important in the context of a governmental mandate.

The Belgian SA issued several other fines or reprimands under the GDPR in 2019:

- On 9 July, the SA issued a reprimand to the Federal Public Service for Health after it failed to respond to the exercise of a citizen's right to data access, despite being ordered to do so by the SA. The decision highlighted the lack of internal procedures enabling the institution to meet the GDPR's requirements.

[1] This non-exhaustive list is based on information received from the national Supervisory Authorities.

- On 17 September, the SA imposed a fine of EUR 10,000 on a retailer for requesting a customer's electronic identity card in order to create a loyalty card; the amount and nature of data were deemed disproportionate to the purposes of the service.
- On 25 November, the SA imposed a fine of EUR 5,000 on a mayor and a municipal officer in two separate cases. The SA found that they improperly used personal information to send political advertisements as part of a re-election campaign during the 2018 local elections. Again, the SA highlighted how individuals in public office need to behave exemplarily with regard to data protection, since this is vital to preserve citizens' trust in democracy.
- On 17 December, the SA imposed a fine of EUR 15,000 on a website specialized in legal news for their noncompliant cookie management and privacy policy.
- On the same day, the SA ruled that a non-profit association had failed to comply with a data subject's access request. The SA imposed a fine of EUR 2,000 and ordered the association to meet the request.

6.2.1.3. Denmark

While in most EU countries national SAs can issue administrative fines, the rules vary in Estonia and Denmark. Having examined and assessed a case, the Danish SA transfers it to the police, who examine whether there is a basis for a charge. Any financial penalty is then decided in court.

On 25 March 2019, the Danish SA proposed to fine taxi company Taxa 4x35 a total of DKK 1.2 million (over EUR 160,000) for violating the GDPR. This was the first time that the Danish SA proposed a fine under the GDPR.

During a 2018 inspection, the Danish SA found that the company had failed to delete its customers' data, which amounted to over 8 million personal data records.

On 11 June 2019, the Danish SA proposed a fine of DKK 1.5 million (over EUR 200,000) on furniture company IDDesign A/S for failing to delete the data of 385,000 customers. The company had in fact stored this data in an old system, failing to update it when the GDPR entered into force. As a consequence, deadlines for deletion were never set.

6.2.1.4. Finland

On 15 February 2019, the Finnish SA ordered financial credit company Svea Ekonomi to correct its practices for the processing of personal data.

This decision resulted from two cases, the first of which arose from a single data subject's complaint and concerned the personal data used to assess creditworthiness and the data subject's right to inspect this data.

The SA also investigated Svea Ekonomi's notification practices related to the automatic decision-making system used to assess creditworthiness, finding that they did not sufficiently explain the logic for data processing to the extent that a credit applicant could understand the grounds for the decision.

6.2.1.5. France

On 21 January, the French SA (CNIL) imposed a financial penalty of EUR 50 million on Google LLC for lack of transparency, inadequate information and lack of valid consent regarding the personalisation of ads. This was the first time that the CNIL issued a fine under the GDPR.

The case arose from group complaints made by two associations in 2018, which challenged Google's legal basis to process its service users' personal data, particularly for ad personalisation purposes.

As Google has its European headquarters in Ireland, the CNIL contacted the other SAs to assess which Supervisory Authority should be considered the LSA.

The European headquarters of Google did not have decision-making powers on the processing operations in the context of the Android system or the services provided by Google when creating an account during the configuration of a mobile phone. Due to these circumstances, the OSS mechanism was not applicable.

Therefore, the CNIL was able to initiate investigations into the compliance of the processing operations implemented by Google with the French Data Protection Act and the GDPR. The CNIL's restricted committee observed two types of breaches of the GDPR:

- **A violation of the obligations of transparency and information**. The information provided by Google was found to be not easily accessible for users. In addition, some information was not always clear nor comprehensive.
- **A violation of the obligation to have a legal basis for data processing for ad personalisation**. It was observed that the users' consent was not sufficiently informed in relation to the extent of data processing. Moreover, the collected consent was neither specific nor unambiguous, as it lacked a clear affirmative action from the user.

The CNIL's restricted committee deemed that these infringements deprived users of essential guarantees regarding processing operations that can reveal important parts of their private life, since they are based on a huge amount of data, a wide variety of services and almost unlimited possible combinations. Moreover, the violations were continuous breaches of the GDPR, rather than one-off, time-limited infringements. In the opinion of the committee, this justified the fine's extent and publicity.

6.2.1.6. Germany

On 30 October 2019, the Berlin SA issued a fine of EUR 14.5 million against Deutsche Wohnen SE for violations of the GDPR. During on-site inspections, the SA found that the company had unnecessarily stored its tenants' personal data without providing the possibility of removing the data. Following a second inspection, the SA found that the company had not made meaningful progress and imposed the fine.

On 3 December, the SA of Rhineland-Palatinate imposed a fine of EUR 105,000 on a hospital for structural technical and organisational deficits in the hospital's patient and privacy management.

At the federal level, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) imposed two fines on telecommunications service providers on 18 December 2019:

- The BfDI imposed a fine of EUR 9,550,000 on 1&1 Telecom GmbH, finding that the company did not provide sufficient technical and organizational measures to prevent unauthorised persons from being able to obtain customer information via the customer hotline service.
- It also imposed a fine of EUR 10,000 on Rapidata GmbH for failing to appoint an internal data protection officer.

6.2.1.7. Greece

In 2019, the Hellenic SA imposed four administrative fines under the GDPR:

- In July, after an investigation into Pricewaterhouse-Coopers Business Solutions, the SA found that the company had processed employees' personal data in an unlawful, unfair and non-transparent manner. As a result, the SA imposed a fine of EUR 150,000 and ordered the company to correct its processing operations to comply with the GDPR.
- On 7 October, the SA imposed two administrative fines amounting to a total of EUR 400,000 on telephone service provider Hellenic Telecommunications Organization (OTE), for failure to implement a number of provisions under the GDPR, namely the principle of accuracy, data protection by design and the right to object.
- In December, after an investigation into ALLSEAS MARINE S.A., the SA found that the GDPR had been infringed. The company had failed to comply with a data subject's request to access his personal data stored on a company computer. As a result, the SA ordered the company to comply with the complainant's request immediately. In addition, it ordered the company to ensure within a month that the processing operations via video devices comply with the GDPR and imposed an administrative fine amounting to EUR 15,000 on the company.

- In December, the SA also imposed a fine of EUR 150,000 on AEGEAN MARINE PETROLEUM NETWORK INC (AMPNI) for GDPR violations with regard to personal data processing operations. In addition, the data controller violated the principles of transparency and of secure processing, due to a lack of appropriate technical and organizational measures, which resulted in the unlawful copying of the entire contents of the company's server.

6.2.1.8. Hungary

The Hungarian SA (NAIH) was notified by a citizen that a webpage operated by a Hungarian parliamentary party, the Democratic Coalition (DK), contained personal data of the party's supporters and was openly accessible via an anonymous hacker forum.

Following a data breach during which an unknown attacker uploaded the data on the internet, DK failed to notify the NAIH or the 6,000 data subjects affected by the breach.

The NAIH ruled that the fact that the concerned data were special categories of personal data revealing political opinions was an aggravating circumstance and issued an administrative fine of HUF 11 million (EUR 32,000).

6.2.1.9. Italy

On 30 April 2019, the Italian SA issued a decision against one of Italy's leading email service providers after the company notified a data breach. On 20 February, technical inquiries had spotted fraudulent access via a WiFi hotspot, which had affected about 1.5 million users.

To limit the data breach consequences, the affected users trying to access their accounts were instructed to change their passwords. Affected users received emails with very limited information on unspecified "unusual activities" in the processing systems, without any reference to a data breach or any indication to take additional measures.

The Italian SA considered the information provided to be insufficient, in the light of the severe risks users had been exposed to, and ordered the company to reissue the communication with a clear description of the type of breach and its possible consequences. The SA also mandated that the company provide users with specific guidance on what measures to take in order to prevent additional risks.

6.2.1.10 Latvia

On 26 August 2019, the Director of the Latvian SA (DSI) imposed a financial penalty of EUR 7,000 against an online retailer for non-compliance with GDPR provisions such as data subjects' right to erasure and non-cooperation with the SA.

The DSI's investigation was initiated after a data subject's complaint that the company had not deleted their personal data despite repeated requests.

6.2.1.11 Lithuania

On 14 May 2019, the Lithuanian SA imposed its first significant fine for breaches of the GDPR. The sanction was imposed on financial services company MisterTango UAB, following a personal data breach in the payment initiation service system, which, among other things, had not been reported to the SA.

As the company owns a branch in Latvia and therefore operates internationally, the Lithuanian SA coordinated with its Latvian counterpart to reach a decision.

Following an investigation, the Lithuanian SA ruled that the company had breached the GDPR's requirements, as it improperly processed personal data in screenshots, made personal data publicly available and failed to report the personal data breach to the SA.

The SA imposed an administrative fine of EUR 61,500. The decision was appealed, but the complaint was rejected by the court of first instance. At the time of publishing this report, the decision was under appeal before the higher court.

6.2.1.12 Malta

In November 2018, the Maltese SA was informed of a

personal data breach on the Lands Authority's online portal, following a report by newspaper The Times of Malta.

The SA's investigation established that the online application platform available on the Authority's portal lacked the necessary technical and organisational measures to ensure secure processing.

On 20 February 2019, the SA found that the Lands Authority had infringed the provisions of the GDPR and issued an administrative fine of EUR 5,000.

6.2.1.13 Norway

On 19 March 2019, the Norwegian SA imposed an administrative fine of NOK 1.6 million, the equivalent of EUR 170,000, on the Municipality of Bergen.

The incident related to computer files in the municipality's computer system, containing the personal data of over 35,000 pupils and employees of the municipality's primary schools. Due to insufficient security measures, these files were unprotected and openly accessible for any system user regardless of type of authorisation.

This enabled unauthorised users to access the school's various information systems and personal data. The fact that the majority of the affected individuals were children and that the municipality was warned several times (both by the authority and by an internal whistleblower) were considered aggravating factors. The municipality did not appeal the decision.

In 2019, the Norwegian SA also imposed two administrative fines on the Municipality of Oslo, which did not appeal their decisions.

- On 11 October, the Municipality's Education Agency was fined EUR 120,000 for failing to implement appropriate security measures in the data processing of a mobile app. The app was used for communication between school employees, parents and pupils.
- On 18 December, the Municipality's Nursing Home Agency was fined EUR 49,300 for having stored patient data from the city's nursing homes and health centres outside the electronic health record system, from 2007 to November 2018.

6.2.1.14 Poland

In 2019, the Polish SA (UODO) issued the following fines under the GDPR:

- On 26 March, the UODO imposed its first fine, amounting to PLN 943,000 (EUR 220,000), for a company's failure to fulfil the information obligation.
- On 20 September, the UODO imposed a fine of PLN 2.8 million (EUR 645,000) on Morele.net for non-compliance with the required technical means of data protection, such as the principle of confidentiality, as set out in Article 5.1.f GDPR.
- On 31 October, the UODO imposed its first administrative fine on a public entity, for an amount of PLN 40,000 (over EUR 9,200). The reason for imposing the fine was that the mayor of the city did not conclude a personal data processing agreement with the entities to which he transferred data.
- On 6 November, the UODO imposed an administrative fine of over PLN 200,000 (over EUR 46,000) on ClickQuickNow for, inter alia, obstructing the exercise of the right to withdraw consent to the processing of personal data.

6.2.1.15 Romania

In 2019, the Romanian SA issued 20 fines for violations of the GDPR:

- On 26 June, the SA issued its first administrative fine under the GDPR, sanctioning bank UniCredit RON 613,912 (EUR 130,000) for its failure to implement appropriate technical and organisational measures to ensure data protection in its processing. As a result, almost 340,000 individuals were exposed to disclosure of their personal data between 25 May and 10 December 2018.
- On 2 July, the SA found that hotel World Trade Center Bucharest had not implemented the necessary measures for secure processing, leading to a leak of clients' personal data. It fined the controller for an amount of RON 71,028 (EUR 15,000).
- On 5 July, the SA fined Legal Company & Tax Hub SRL RON 14,173.50 (EUR 3,000), for failure to implement adequate technical and organisational measures to ensure secure data processing.
- In July, the SA also imposed an administrative fine of

RON 11,834.25 (EUR 2,500) on Utties Industries SRL, for failure to comply with secure data processing in the context of video devices and employees' personal identification numbers.

- On 28 October, the SA finalised its investigation into controller Fan Courier Express, and found that it did not implement adequate technical and organizational measures to ensure protection of data in its processing. As a result, the company was fined RON 52,325.90 (EUR 11,000).
- On 31 October, the SA imposed three administrative fines. The first, amounting to EUR 9,000, was imposed on Inteligo Media for failing to prove that it had obtained explicit consent for data processing from over 4,000 users. The SA also imposed two fines, EUR 150,000 and EUR 20,000 respectively, on Raiffeisen Bank and Vreau Credit, as it found that the two controllers had unlawfully exchanged clients' personal data in order to determine their eligibility for credit.
- On 4 November, the SA issued a fine against ING Bank's Bucharest branch for failing to ensure compliance with the principles of privacy by design and by default in the settlement process of card transactions affecting over 225,000 customers. The sanction amounted to EUR 80,000.
- On 7 November, air transport company Tarom was fined RON 95,194 (EUR 20,000), due to failure to implement the necessary measures to ensure secure data processing, which resulted in a data breach.
- On 18 November, the SA fined Royal President SRL RON 11,932.25 (EUR 2,500), for failing to grant the right of access within the time limit and for unauthorised disclosure of personal data.
- On 19 November, Globus Score SRL was fined RON 9,551.80 (EUR 2,000) for failing to comply with the SA's request of information, following the opening of an investigation.
- On 25 November, the SA fined Telekom Romania Mobile Communications RON 9,544.40 (EUR 2,000) for failing to keep its customers' personal data accurate, up-to-date and confidential.
- On 29 November, an association of owners was fined RON 2,389.05 (EUR 500) and issued with two reprimands for unlawful accessing personal images from a video surveillance system.
- On 2 December, the SA issued three administrative fines. The Bucharest branch of BNP Paribas Personal Finance was fined RON 9,508 (EUR 2,000) after complaints that it had failed to delete personal data within the required time limit. The SA also fined controllers Modern Barber SRL and Nicola Medical Team 17 SRL for failing to comply with the SA's request of information. The sanctions amounted to RON 14,329.50 (EUR 3,000) and RON 9,555.40 (EUR 2,000) respectively.
- On 10 December, the SA fined Hora Credit IFN SA a total amount of RON 66,901.80 (EUR 15,000). The controller processed personal data without verifying and validating its accuracy, and failed to maintain its confidentiality.
- On 13 December, company Entirely Shipping & Trading SRL was fined a total amount of RON 47,786 (EUR 10,000) for several violations of the GDPR, including legitimate interest in the context of video surveillance, lack of adequate data protection policies and unlawful processing of biometric data.
- On 16 December, the SA imposed an administrative fine of RON 14,334.30 (EUR 3,000) on SC Enel Energie SA, for failing to comply with the data subject's right to consent and object to the processing of their personal data.

6.2.1.16 Spain

On 17 October, the Spanish SA fined the company Vueling a total of EUR 30,000 for its website cookie policy.

While users accessing the website were informed about the general cookie policy, the company did not provide a management system or cookie configuration panel allowing the user to delete cookies in a granular way.
Besides violating the GDPR, these circumstances were also an infringement of the Spanish Law on Information Society Services and Electronic Commerce, which requires that users give explicit consent to any use of data storage and retrieval devices.

6.2.1.17 Sweden

On 22 August 2019, the Swedish SA issued its first financial penalty under the GDPR. The SA fined a municipality SEK 200,000 (approximately EUR 20,000) for using facial recognition technology to monitor school students' attendance.

The SA found that the school processed sensitive biometric data unlawfully and failed to conduct an adequate impact assessment, including seeking prior consultation with the SA. In addition, although the processing was based on consent, the SA considered it did not have a valid legal basis given the clear imbalance between the data subject and the controller.

On 18 December 2019, the Swedish SA issued an administrative fine of EUR 35,000 EUR against Mrkoll.se, a website that publishes the personal data of all Swedes above the age of 16 (over 8 million people). In Sweden, websites which are granted publishing certificates have a constitutional protection for the majority of their activities, meaning that the GDPR does not apply under those circumstances.

However, the SA found that some of the data published by the website fell under special categories, such as credit information and criminal records. This required the SA's authorisation, which had not been issued.

6.2.1.18 United Kingdom

On 20 December 2019, the UK SA (ICO) fined a London-based pharmacy GBP 275,000 (EUR 315,000) for failing to ensure the security of special category data.

The pharmacy, Doorstep Dispensaree Ltd, which supplies medicines to customers and care homes, left approximately 500,000 documents in unlocked containers in its premises. The documents included names, addresses, dates of birth, NHS numbers, medical information, and prescriptions belonging to an unknown number of people.

The ICO launched its investigation after it was alerted to the insecurely stored documents by the Medicines and Healthcare Products Regulatory Agency, which was carrying out its own separate enquiry.

In addition to the fine, Doorstep Dispensaree was issued with an enforcement notice due to the significance of the violations and was ordered to improve its data protection practices within three months.

6.3. SA SURVEY ON BUDGET AND STAFF

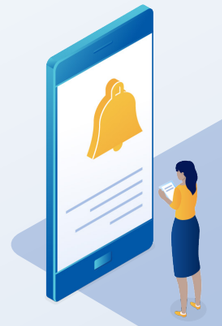
Under the GDPR, SAs have received new harmonised tasks and powers. They wield greater enforcement and investigation powers, handle individuals' complaints, promote awareness on data protection law, and cooperate with the other SAs. This implies a need for increased budgets and more staff members.

In the context of the evaluation of the GDPR, the EDPB conducted a survey among the SAs about their budget and staff. Most of SAs stated that resources made available to them are insufficient.

The EDPB surveyed Supervisory Authorities in the context of the review of the GDPR. While an increase in the 2019 budget occurred in 27 cases, most SAs found available resources insufficient.

Based on information provided by SAs from 30 EEA countries, an increase in the budget for 2019 occurred in 27 cases. The remaining three SAs saw their budget decrease.
According to the same survey, a majority of SAs (22) increased their staff numbers in 2019. Five SAs reported that the number of their employees did not increase from 2018 to 2019, while three SAs saw a decrease in staff numbers. Differences in personnel requirements across SAs are to be expected, given the varied remits of the SAs.

The EDPB also collected similar information upon request from the European Parliament's LIBE committee. This report is available on the EDPB's website.



7

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

In October 2018, Regulation 2018/1725 on the protection of personal data processed by EU institutions and bodies was adopted.

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

In December 2019, the Coordinated Supervision Committee was formally established within the EDPB. It brings together EEA SAs and the EDPS as well as SAs from non-EU Schengen Member States, where foreseen under EU law.

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

Participation in the Committee meetings can occur under

various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act.

During its first meeting, the Committee elected Giuseppe Busia from the Italian SA as Coordinator and Iris Gnedler from the German Federal SA as Deputy Coordinator for a term of two years, and adopted its Rules of Procedure.

Article 62 of Regulation 2018/1725 outlines the Committee's supervision of IT systems, bodies, offices, and agencies in the following fields:

1. **Border, Asylum and Migration**:
    a. Schengen Information System (SIS), ensuring border control cooperation;
    b. Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Schengen States;
    c. European Travel Information and Authorization System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone;
    d. Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States.
2. **Police and Justice Cooperation**:
    a. SIS, which also ensures law enforcement cooperation;
    b. European Public Prosecutor Office (EPPO);
    c. Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States;
    d. European Criminal Records Information System on third-country nationals (ECRIS-TCN), which allows Member States' authorities to identify which other Member States hold criminal records on third-country nationals or stateless persons being checked.
3. **Internal Market**: IMI system, which allows exchange of information between public authorities involved in the practical implementation of EU law.

In 2019, the Committee was in charge of the coordinated supervision of the IMI system and Eurojust. In 2020, this will be extended to include EPPO. In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the Committee.

8

Main objectives for 2020

8.1. LEGAL WORK PLAN

At the beginning of 2019, the EDPB adopted a two-year work programme for 2019-2020. This is based on the priorities set by all stakeholders, including the EU legislator, as identified by the EDPB members. Three areas of interest were identified, as outlined below.

By the end of 2019, halfway through its work plan, the EDPB made significant progress across its stated objectives and is advancing towards completing them in its second working year.

8.1.1 Guidance

The EDPB will continue issuing Guidelines to ensure consistent interpretation of the GDPR across the EU, enabling stakeholders and Supervisory Authorities (SAs) to apply the GDPR's provisions in a harmonised manner.

In 2019, the EDPB issued guidance related to the provision of online services to data subjects, as well as video devices, search engine delisting and data protection by design and by default.

In 2020, the EDPB will aim to provide guidance on data controllers and processors, data subject rights and the concept of legitimate interest. It will also intensify its work in the context of advanced technologies, such as connected vehicles, blockchain, artificial intelligence, and digital assistants.

In addition to the work outlined in the work plan, in 2020, the EDPB is to provide guidance on the implications for data protection in the context of the fight against COVID-19, both on its own initiative and upon consultation by the European Commission.

8.1.2 Advisory role to the European Commission

The EDPB will continue to advise the European Commission on issues such as cross-border e-Evidence data access requests, the revision or adoption of adequacy decisions for data transfers to third countries and any possible revision of the EU-Canada Passenger Name Record (PNR) agreement.

8.1.3 Consistency findings

In cross-border cases where consensus between the Lead SA and Concerned SAs within the relevant cooperation procedure cannot be reached, the EDPB will act as a dispute resolution body and issue binding decisions.

In addition, the EDPB will continue to deliver Consistency Opinions to SAs in line with Article 64 GDPR. These include any relevant draft decision from competent SAs on issues such as cross-border data transfers, Binding Corporate Rules and standard or ad-hoc contractual clauses.

The EDPB will also deliver accreditation requirements for code of conduct monitoring bodies, as well as certification bodies to enable the finalisation of the national legal framework and the use of these accountability tools in practice.

8.2. COMMUNICATIONS

The EDPB aims to foster full transparency around its work and activities among media, the public and stakeholders within the public and private sectors.

2019 saw an even greater public focus on data protection and privacy issues. The first full year of the GDPR being in application generated considerable discussion among stakeholders and citizens around the importance of data subject rights. It also increased public awareness of issues such as consent, legitimate interest and lawful processing of data.

To respond to this increased level of interest and address stakeholder concerns about the application of the GDPR, the EDPB has been actively engaging with all relevant parties, through workshops, surveys and informational events. In 2020, the EDPB will deepen existing stakeholder relationships and develop new ones.

The EDPB will continue issuing Guidelines to ensure consistent interpretation of the GDPR, advise the European Commission and deliver Consistency Opinions to Supervisory Authorities.

The EDPB Members, including its Chair and Deputy Chairs, are fully committed to continuing their participation in relevant conferences and speaking engagements.

The EDPB Secretariat will continue to ensure a harmonised communication approach. This includes continuing to drive public engagement with the EDPB's activities through its social media presence, as well as enhancing cooperation with SAs. To this end, the EDPB will maintain and strengthen the network of SAs' press and communications officers.

9

Annexes

9.1 GENERAL GUIDANCE ADOPTED IN 2019

1. *Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725)*
2. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation*
3. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects – version adopted after public consultation*
4. *Guidelines 3/2019 on processing of personal data through video devices – version adopted after public consultation*
5. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – version for public consultation*
6. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) – version for public consultation*

9.2 CONSISTENCY OPINIONS ADOPTED IN 2019

- *Opinion 1/2019 on the draft list of the competent supervisory authority of the Principality of Liechtenstein regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*
- *Opinion 2/2019 on the draft list of the competent supervisory authority of Norway regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*
- *Opinion 4/2019 on the draft Administrative Arrangement for the transfer of personal data between European Economic Area ("EEA") Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities*
  - *Draft administrative arrangement for the transfer of personal data*
- *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*
- *Opinion 6/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*
- *Opinion 7/2019 on the draft list of the competent supervisory authority of Iceland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*
- *Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment*
- *Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR*
- *Opinion 10/2019 on the draft list of the competent supervisory authority of Cyprus regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35(4) GDPR)*
- *Opinion 11/2019 on the draft list of the competent supervisory authority of the Czech Republic regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)*
- *Opinion 12/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)*
- *Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)*
- *Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)*
  - *DK SA Standard Contractual Clauses for the purposes of compliance with art. 28 GDPR*
- *Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc.*
- *Opinion 16/2019 on the draft decision of the Belgian Supervisory Authority regarding the Binding Corporate Rules of ExxonMobil Corporation*
- *Opinion 17/2019 on the UK data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR*

9.3. JOINT OPINIONS ADOPTED IN 2019

- *EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI)*

9.4. LEGISLATIVE CONSULTATION

- *Second Annual Joint Review report on the EU-US Privacy Shield*
- *Third Annual Joint Review report on the EU-US Privacy Shield*
- *Opinion 3/2019 on the interplay between the Clinical Trials Regulation (CTR) and the GDPR*
- *Statement 3/2019 on an ePrivacy regulation*
- *Contribution to the draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)*

9.5. OTHER DOCUMENTS

- *Information note on data transfers under the GDPR in the event of a no-deal Brexit*
- *Statement 1/2019 on the US Foreign Account Tax Compliance Act (FATCA)*
- *EDPB LIBE report on the implementation of GDPR*
- *EDPB pleading before the CJEU in Case C-311/18 (Facebook Ireland and Schrems)*

EDPB Annual Report 2019

9.6. LIST OF EXPERT SUBGROUPS WITH SCOPE OF MANDATE

NAME OF SUBGROUP	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. EU-US Privacy Shield) • Passenger Name Records (PNR) • Border controls • Preparation of the coordinated supervision under Art. 62 1725/2018
Compliance, e-Government and Health Expert Subgroup	• Code 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
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 SUBGROUP	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 Fining TF
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 SUBGROUP	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 Compliance Tools ESG, Enforcement ESG and Technology ESG) and IX
Social Media Expert Subgroup	• Analyzing social media services, conceived as online platforms that focus on enabling the development of networks and communities of users, among which information and content is shared and whereby additional functions provided by social media services include targeting, personalisation, application integration, social plug-ins, user authentication, analytics and publishing • 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 SUBGROUP	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 ESGs

Contact details

Postal address:
Rue Wiertz 60, B-1047 Brussels

Office address:
Rue Montoyer 30, B-1000 Brussels

Email:
edpb@edpb.europa.eu

@eu_edpb
eu-edpb
edpb.europa.eu

edpb
European Data Protection Board