SAFEGUARDING INDIVIDUALS' DIGITAL RIGHTS

edpb
European Data Protection Board

ANNUAL REPORT 2023

TABLE OF CONTENTS

FOREWORD

I am pleased to present the European Data Protection Board's (EDPB) 2023 Annual Report. In this report, you will find details about the EDPB's achievements and milestones, during another transformative year for the Board. 2023 was my first year as Chair of the EDPB, a role I took over from Andrea Jelinek. I would like to thank Andrea once more for her expert leadership and unyielding commitment, which helped shape the EDPB.

Today, the EDPB is a unique body with great responsibilities and far-reaching impact. We have built an impressive compendium of guidelines, created new cooperation methods for the authorities, and adopted significant decisions to ensure that authorities apply the GDPR in a correct and consistent manner. We also worked a lot to raise awareness of the GDPR at the European and international levels, so that individuals know their rights and exercise them, and that companies, even small ones, can understand how to comply with their legal duties.

In 2023, notable achievements include the launch of our Data Protection Guide for Small Business (April), a user-friendly website offering guidance and practical suggestions and helping to navigate the many resources Data

Protection Authorities (DPAs), at national level, have created on the GDPR.

The binding and urgent binding decisions we adopted in 2023 gave important common interpretations of data protection law and key legal principles that shape the digital landscape, for example on the international transfers of personal data (April), on unfair design practices of social media apps targeting children (August) or on the behavioural advertising practices of social media networks (October). They also led, often, to very large fines imposed by the Lead Supervisory Authorities.

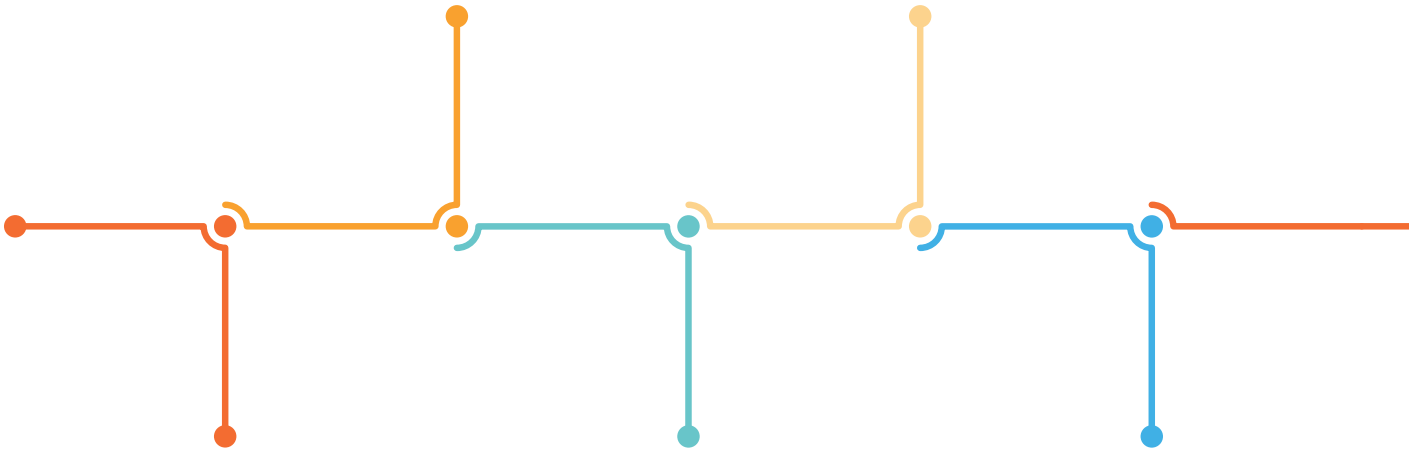
We continued to build and expand our enforcement cooperation methods, to ensure that DPAs can enforce more effectively. In March, we launched our second Coordinated Enforcement Framework action, this time focusing on the very important role DPOs have in ensuring organisations' compliance with the GDPR. We also gave input to the European Commission's draft Regulation to harmonise administrative procedures, which - once implemented - can be a leap forward in overcoming obstacles to cooperation between authorities and enforcement (September).

The European Union continues to take on a pioneering role in regulating technology with a cluster of new laws like the Digital Markets Act, the Digital Services Act and the Artificial Intelligence Act, which build on the foundations of data protection legislation. As I write this, we are in the process of shaping our new Strategy. It will help us face the many challenges that lie ahead of us, so that the EDPB can continue to ensure that technologies and the digital economy are in line with our values and fundamental right of data protection.

Anu Talus

Chair of the European Data Protection Board

HIGHLIGHTS 2023



FEBRUARY 28

Opinion 5/2023 on the draft adequacy decision regarding the EU-U.S. Data Privacy Framework

MARCH 15

Launch of the 2023 Coordinated Enforcement Action, focusing on the designation and position of Data Protection Officers

APRIL 27

Launch of the EDPB Data Protection Guide for Small Business

MAY 22

€1.2 billion fine to Meta Ireland Limited issued by the Irish DPA following the EDPB's Binding Decision 1/2023

MAY 25

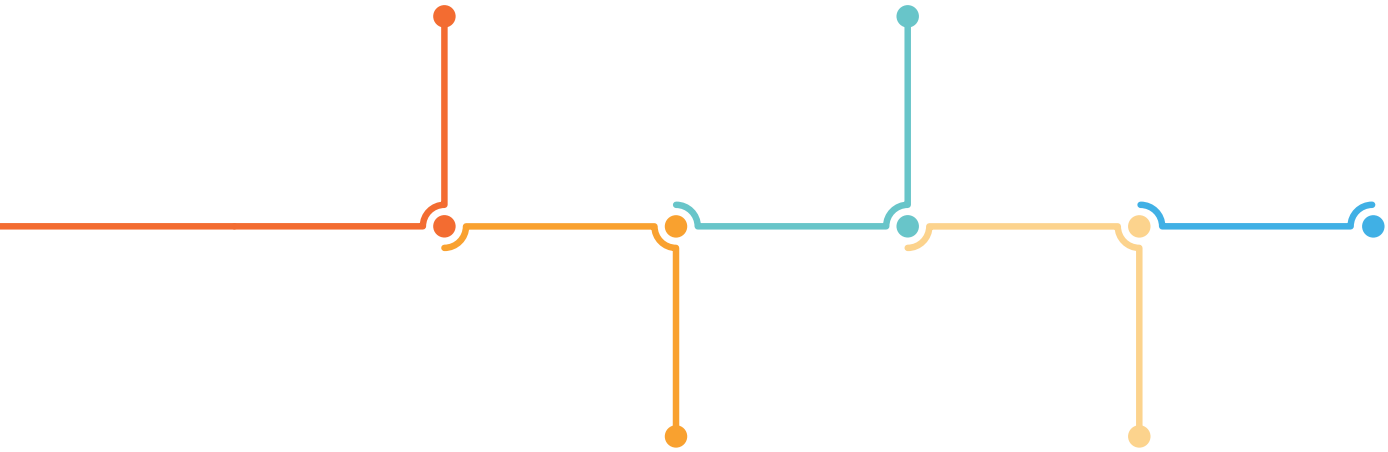
Election of Anu Talus as the new Chair and Irene Loizidou Nikolaidou as the new Deputy Chair

SEPTEMBER 15

€345 million fine against TikTok Technology Limited by the Irish DPA, following EDPB's Binding Decision 2/2023

OCTOBER 27

Urgent Binding Decision 01/2023 instructing the Irish DPA to take, within two weeks, final measures regarding Meta Ireland Limited



SEPTEMBER 19

EDPB/EDPS joint opinion on a Proposal for a Regulation laying down additional procedural rules relating to the enforcement of the GDPR

DECEMBER 12-13

Contribution to the European Commission's report on the application of the GDPR under Art. 97

1. THE EDPB SECRETARIAT

The EDPB Secretariat - At the heart of the EDPB

2023 has been another remarkable year for the EDPB and the EDPB Secretariat, with landmark binding decisions, a series of initiatives to boost enforcement cooperation, important guidelines and opinions on draft legislation, the launch of our Data Protection Guide for Small Business, and not in the least: the election of Anu Talus as the new EDPB Chair.

I am proud to say that, over the years, the EDPB Secretariat has established itself as a robust, widely respected and dynamic organisation. The Secretariat has gone through a considerable evolution since its establishment. Back in 2018, we started off with a dozen professionals, mainly providing logistical and administrative support to the Board, while today we are a group of highly specialised and dynamic individuals, organised in 5 sectors, working together for a common goal. We are fully committed to making sure the GDPR delivers.

However, there is a vital need for more resources to ensure that the EDPB can continue to fulfil its missions and comply with its legal duties.

The EDPB Secretariat supports the Board in drafting binding decisions and in defending the EDPB in Court. It also contributes to the preparation of other EDPB documents, such as guidance and legal advice on new legislative proposals. It disseminates this work to the public, ensures press relations for the EDPB, and supports the Chair in her role of

representing the Board. The EDPB Secretariat also develops and runs the EDPB's IT tools which are used by approximately 1,500 staff members of EEA supervisory authorities. It organised over 360 EDPB meetings in 2023, during which members prepare the EDPB documents aimed at a consistent application of data protection laws in Europe.

It is no exaggeration to say that the EDPB Secretariat is essential to the work of the EDPB.

However, we face increasing challenges as the number of our tasks is growing. The EDPB Secretariat is now providing the secretariat of the Coordinated Supervisory Committee, which ensures coordinated supervision of large scale IT systems and EU bodies and agencies. In 2023, this activity extended to the supervision of the Schengen Information System, in addition to the Europol, EPPO, Eurojust and IMI that were already falling under the framework of the EDPB activities. Besides, as enforcement picks up speed at national level, so does the EDPB Secretariat's work to prepare an increasing number of Binding Decisions and handle litigation actions related to them.

In the last six years, the EDPB has done a great deal to ensure guidance, consistency, building a framework for the new compliance tools, such as codes of conduct and certification mechanisms and promote cooperation on enforcement and I am confident we will continue to evolve to face the challenges presented by GDPR implementation.

Isabelle VEREECKEN

Head of the EDPB Secretariat

1.1. MISSION AND ACTIVITIES IN 2023

The EDPB Secretariat offers analytical, administrative and logistical support to the EDPB. In practice, the EDPB Secretariat drafts guidelines, legal advice and binding decisions, provides IT solutions to ensure secured and transparent communications between all the European national Data Protection Authorities (DPAs), handles media relations, and organises meetings.

The terms of cooperation between the EDPB and the EDPS are established by the Memorandum of Understanding. The EDPS employs the staff at the EDPB Secretariat. However, they work exclusively under the instructions of the Chair of the EDPB. A dedicated title exists in the EDPS budget to cover both the budget of the EDPB Secretariat and of the EDPB as a whole (e.g., meeting costs, translation and interpretation costs). It includes the 46 staff members who work within the EDPB Secretariat or within the EDPS for the support provided to the EDPB via horizontal administrative services.

The EDPB Secretariat provides analytical and legislative support to the Board. As such, in 2023, the EDPB Secretariat led the drafting of ten opinions, two guidelines and three binding decisions, and contributed to a further fourteen opinions.

The EDPB Secretariat also supports the EDPB in enforcing data protection laws. The EDPB ensures consistent enforcement and promotes cooperation amongst DPAs. For a small number of complex cases on which DPAs cannot agree via consensus, the EDPB adopts binding decisions. The EDPB Secretariat, as the neutral party among DPAs, supports the EDPB with the drafting of these decisions.

In addition, the EDPB Secretariat provides the Secretariat of the Coordinated Supervision

Committee (CSC). The CSC ensures the coordinated supervision of large scale IT systems and of EU bodies, offices and agencies, in accordance with Art. 62 of Regulation (EU) 2018/1725 or with the EU legal act establishing the large scale IT system or the EU body, office or agency.

The EDPB budget forms part of the broader budget of the EDPS. In 2023, the budget of the EDPB amounted to €7.67 million. This budget supports the growth of enforcement and litigation activities, and covers expenditure for EDPB meetings at the plenary and subgroup level, translation and interpretation costs, IT services, and remuneration of the EDPB Secretariat staff. An amending budget of +€300,000 was granted during 2023 due to the significant increase in litigation activities.

In 2023, the EDPB was involved as a party in 12 cases before the CJEU, of which 10 were submitted in 2023,[1] one at the end of 2022[2] and one in 2021.[3] The vast majority of the cases concerned applications for annulment against Binding Decisions adopted by the EDPB.[4]

In the context of these proceedings, the Secretariat of the EDPB worked closely with external lawyers throughout the different stages of the proceedings, including in relation to defining the EDPB's defence strategy and drafting procedural documents.[5]

In addition, the EDPB was also involved as an intervener in one case,[6] in support of the EDPS.

In accordance with Art. 32(2) of the EDPB Rules of Procedure (RoP), the EDPB Secretariat prepares the answers to access requests of EDPB documents which are handled and signed by the Chair or one of the Deputy Chairs. In 2023, the EDPB Secretariat received 39 public access requests for documents held by the EDPB. Confirmatory applications were received in two cases. A single complaint regarding an EDPB confirmatory decision for a request for access to documents was brought to the attention of the European Ombudsman in 2023. This complaint was about the EDPB's refusal to grant access to an assessment of the use of X (Twitter) by DPAs and the EDPB, including one annex. Following a reassessment of the two documents at issue, the EDPB decided to fully disclose them to the applicant. With the complaint being settled, the Ombudsman closed this inquiry and commended the EDPB for its decision in this case.

[1] T-183/23 Ballmann v European Data Protection Board; Joined cases T-70/23, T-84/23, 111/23 Data Protection Commission v European Data Protection Board; T-128/23 Meta Platforms Ireland v European Data Protection Board; T-129/23 Meta Platforms Ireland v European Data Protection Board; T-153/23 WhatsApp Ireland v EDPB; T-325/23 Meta Platforms Ireland v European Data Protection Board; T-1030/23 Tiktok Technology v European Data Protection Board and C-97/23 P WhatsApp Ireland v EDPB.

[2] Case T-682/22 Meta Platforms Ireland v EDPB.

[3] Case T-709/21 WhatsApp Ireland v European Data Protection Board. In 2023, the EDPB dealt with the procedural aftermath of the Order of the General Court of 7/12/2023.

[4] In particular, 10 cases concerned actions for annulment against EDPB's binding decisions, one case concerned access to the file and another case concerned an appeal lodged by a controller before the ECJ following a General Court order that dismissed that controller's request for annulment of an EDPB binding decision.

[5] For instance, the EDPB defence for 3 cases, the rejoinder for 2 cases and the application under Article 130(1) of the Rules of Procedure of the General Court in 4 cases.

[6] C-413/23 P EDPS v SRB.

In the context of the cooperation between DPAs, the EDPB Secretariat provides continuous support to DPAs with IT solutions that facilitate their communication. The EDPB Secretariat also leads the IT Users Expert Subgroup, which coordinates the information systems used by the EDPB, including the Internal Market Information (IMI) system. The Secretariat also replies to requests for support from the DPAs.

The IMI system is essential for the GDPR cooperation among EDPB members. This year, the system facilitated more than 4,580 procedures. There were 419 support requests related to the use of IMI. Overall, the EDPB Secretariat handled a total of 3,418 support enquiries across all EDPB IT systems.

In 2023, IMI celebrated its 15th anniversary. Over time, the system has proven its value and over again for cooperation in different policy fields in the EU.

2023 - a new version of IMI

In 2018, the EDPB opted for IMI as an information exchange system between DPAs, customising and adapting it to their needs in the record time of six months. 19 different procedures were implemented enabling the DPAs to enforce the GDPR.

Since then, IMI has proven to be a robust, flexible and efficient platform that is essential for the GDPR cooperation and enforcement.

With the help of the European Commission, the EDPB continuously improves IMI, enhancing its features to accommodate the new needs of the DPAs.

To enhance the user experience and streamline the workflows, in 2023 an upgraded version of the IMI user interface was introduced, featuring innovative functionalities, such as a more intuitive dashboard allowing easier access and monitoring of ongoing procedures, an improved search functionality, streamlined navigation and improved layout for easier access to key features, and a refreshed visual design. In addition, tutorial videos were made by the EDPB Secretariat to help DPAs master the new IMI features.

A pilot solution was also developed with the help of the European Commission as system provider to interconnect DPAs' national case management systems with IMI. This integration will facilitate the automatic transmission of cases between national systems and IMI, reducing the need for manual data entry and facilitating the tracking of procedures in IMI and national case management systems. In 2023, the feature was successfully tested in France and Spain and it will be further rolled out across the EU upon request.

EDPB HUB, EDPB's primary platform for information sharing with their members, saw significant activity. Over 7,503 different content types were created. This includes 1,496 new pages, 4,787 documents, and 1,014 exchanges. The platform is widely used across various authorities, supporting a substantial user base of over 1,400 members.

The EDPB Secretariat also ensured the continued usability of the EDPB website. The website was visited 275,582 times in 2023 and the most clicked topics were Guidelines, Recommendations, Best Practices, Our members, News, Our documents and Approved Binding Corporate Rules.

An important awareness raising action in 2023 for which the EDPB Secretariat took the lead was the publication of the Data Protection Guide for Small Business. The Guide is a key initiative in the EDPB's 2021-2023 Strategy. It aims to provide practical information to SMEs about GDPR compliance in an accessible and easily understandable language. The main goal of the guide is to help raise awareness of the GDPR among SMEs and to facilitate compliance. The development of tools providing practical, easily understandable and accessible data protection guidance is key to reaching a non-expert audience and promoting data protection in practice.

"Rolling out the actions of national authorities on a European scale increases the impact of awareness-raising initiatives. Thanks to the Data Protection Guide for Small Business, businesses throughout Europe can find answers to their practical questions and ready-to-use tools to help them."

Cédrine Morlière, Head of the Belgian DPA

The EDPB processes personal data according to the rules laid down in Regulation 2018/1725 on the processing of personal data by the Union institutions, bodies, offices and agencies. In accordance with Art. 43 of this Regulation, the EDPB has its own DPO team, which is part of the EDPB Secretariat. In 2023, the EDPB received five data subject requests made on the basis of rights enshrined in Art. 17 to Art. 24 of Regulation 2018/1725. The EDPB Secretariat also provided assistance with replying to individual requests for information involving the processing of their personal data, and supported in handling two data breaches under Arts. 34 and 35 of Regulation 2018/1725 which required a notification to the EDPS.

1.2. RE-ORGANISING THE SECRETARIAT IN 2023

In the past year, the volume and complexity of the EDPB's tasks substantially increased and, in parallel, the role of the EDPB Secretariat evolved. Following the changes made in early 2023, the EDPB Secretariat is now composed of five sectors. This structural improvement was necessary to address the growing workload of the EDPB Secretariat.

The EDPB Secretariat consists of two legal sectors working on drafting binding decisions, litigation and providing analytical support to the EDPB, as well as an information and communications sector, which plays an essential role in presenting the EDPB's work to the outside world or preparing awareness-raising tools, such as the EDPB Guide for Small Business. In addition, the administrative sector and the IT sector provide logistical and IT support to the EDPB.

EDPB SECRETARIAT | ORGANISATIONAL CHART

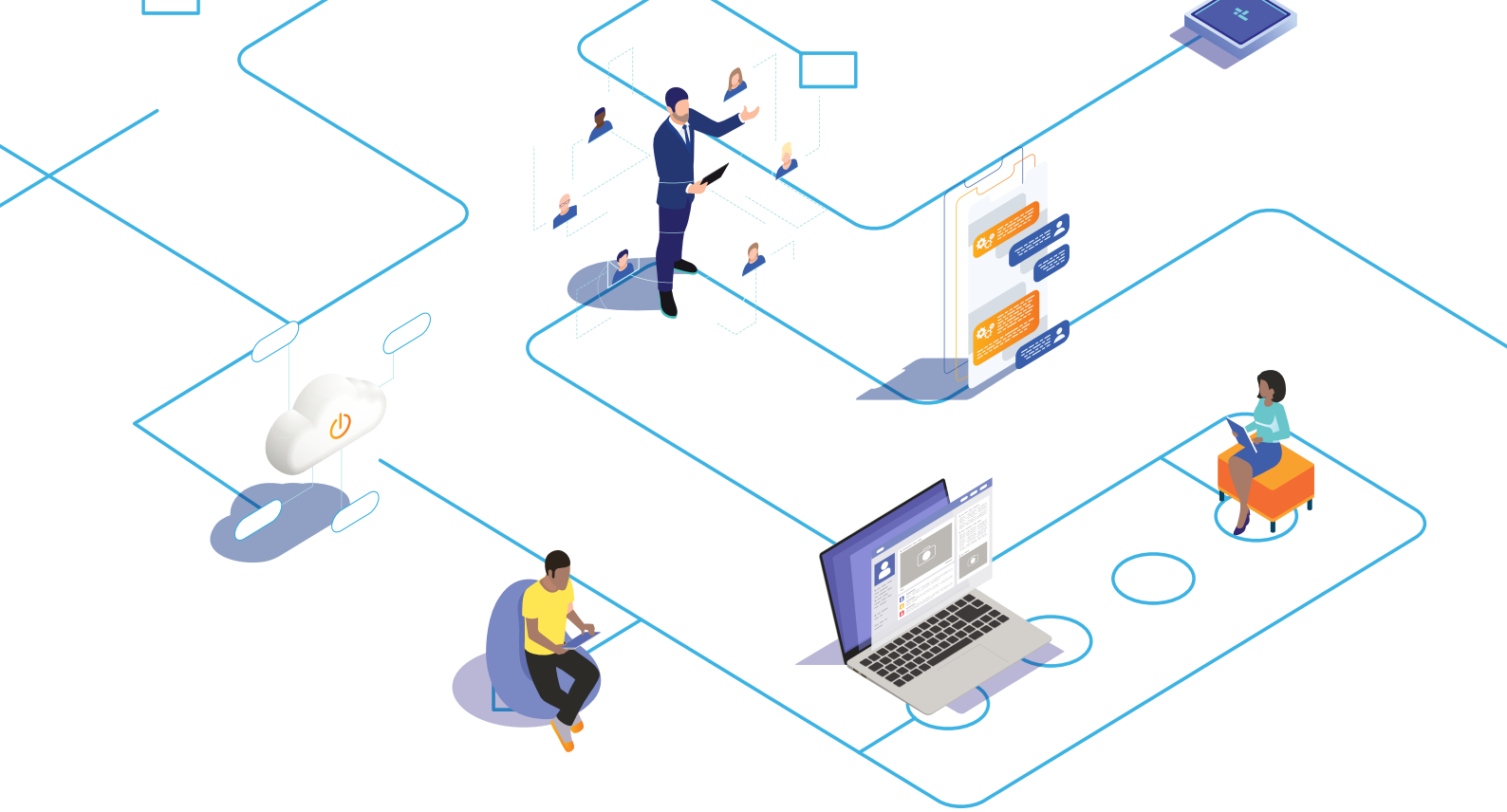
UNIT

Head of EDPB Secretariat
Isabelle VEREECKEN

Deputy Head of EDPB Secretariat
Gwendal LE GRAND

HEADS OF SECTOR

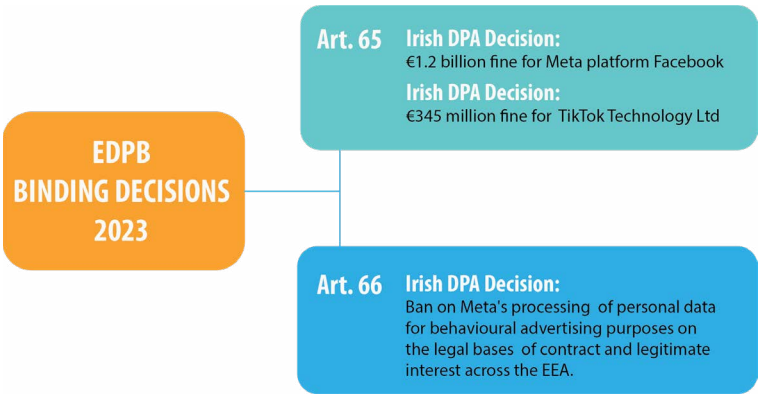
Myriam GUFFLET	Carolina FOGLIA	Greet GYSEN	Effrosyni PANAGOU	Ahmed IMMOUN
Litigation and international affairs	Legal affairs-cooperation and enforcement	Information and communication	Administrative matters	IT matters



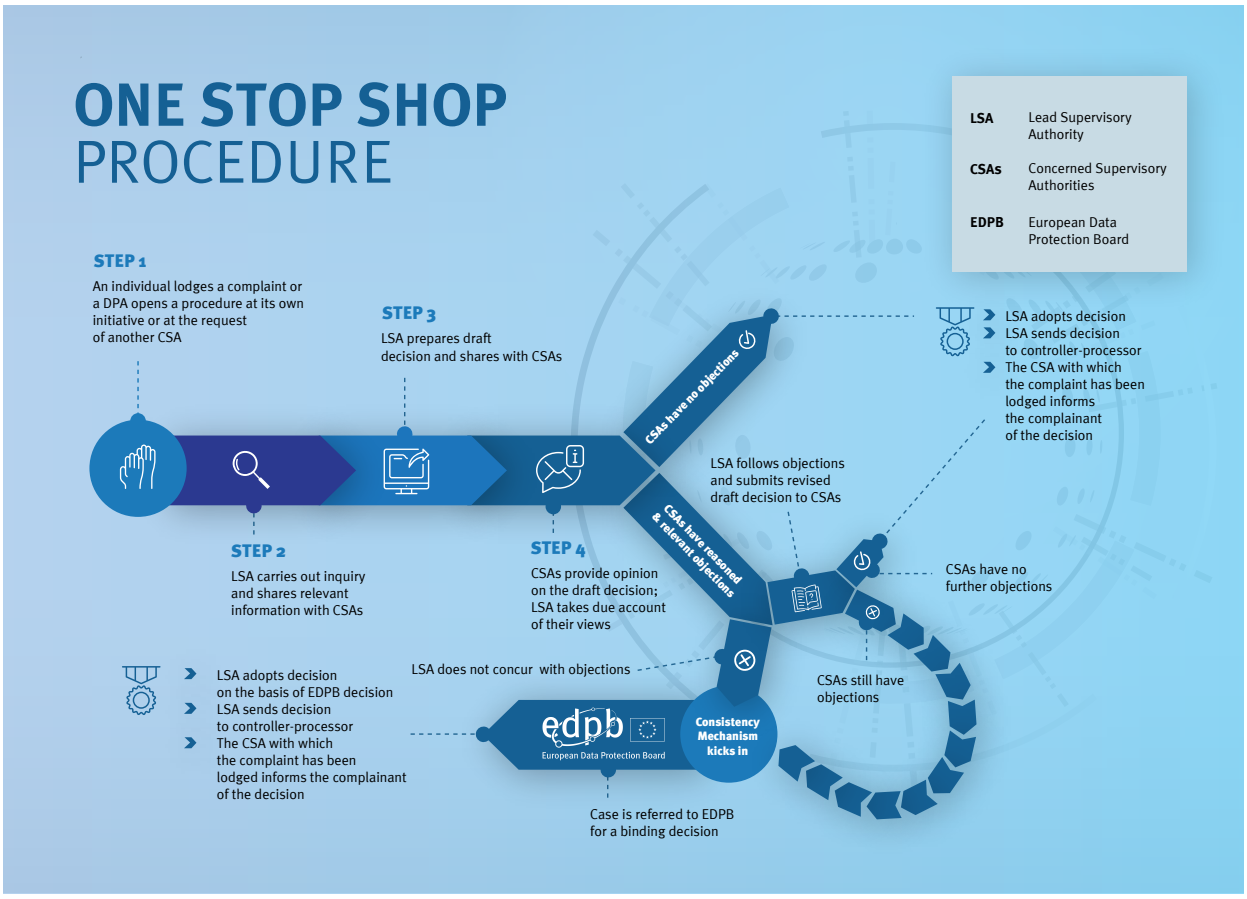
2. EUROPEAN DATA PROTECTION BOARD - ACTIVITIES IN 2023

2.1. BINDING DECISIONS

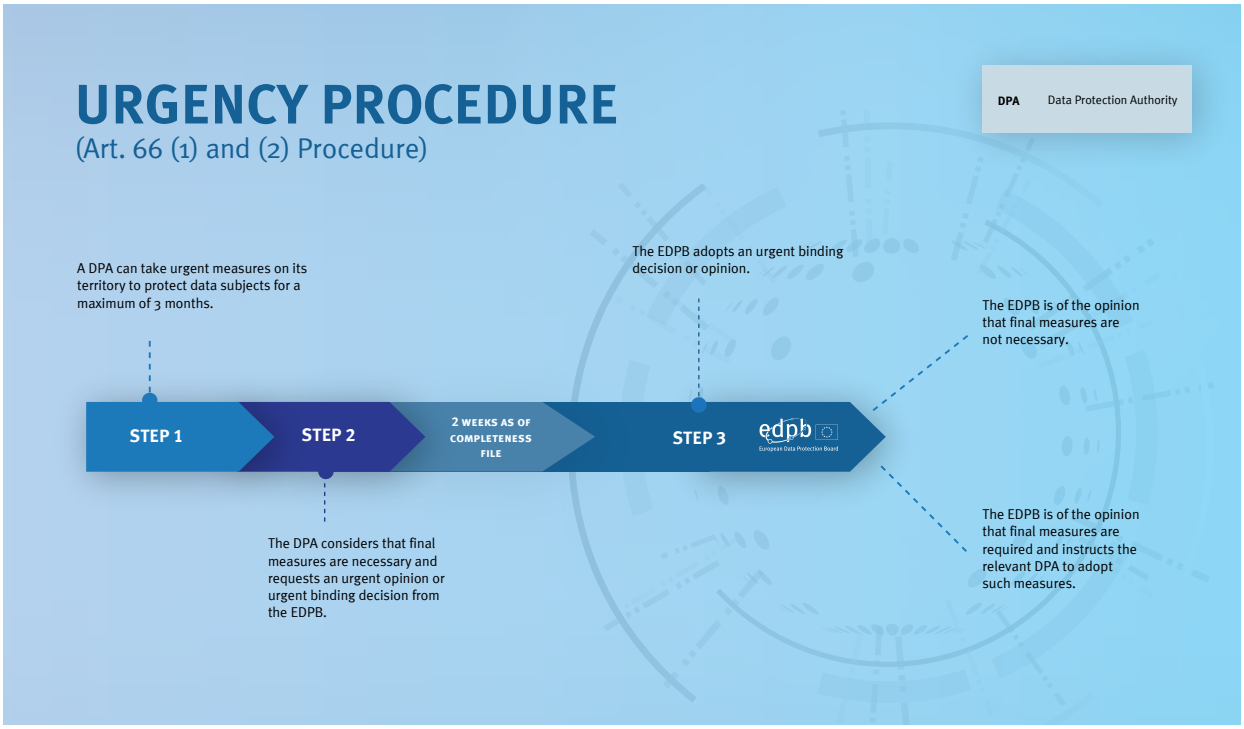
Enforcing the GDPR and issuing fines is the competence of DPAs. They do so at national level and in cross-border cases, for which they cooperate, through the One-Stop-Shop (OSS) system. In instances where DPAs are unable to reach a consensus, the EDPB adopts a decision pursuant to Art. 65 GDPR. The decision is binding towards the lead DPA, thereby compelling it to adjust its decision accordingly. Approximately 1% of OSS decisions have been going through the dispute resolution mechanism. These decisions often concern major players and the processing of data of all European individuals. Since 2018, LSAs handed out over €2.5 billion in fines after a binding decision. This represents around 55% of the total amount of fines issued since 2018.



See pages 16 - 19 for the full summary of binding decisions adopted in 2023.



In exceptional cases, urgent binding decisions may be adopted by the EDPB in line with Art. 66 GDPR. This urgency procedure has been put in place to ensure consistency in the enforcement of the GDPR and may only be triggered by authorities in situations where an urgent need to act is determined.



Binding decisions are drafted by the EDPB Secretariat, in close collaboration with the Members, before they are adopted by the Board. They often set a precedent by settling disputes on key legal issues and, at the same time, fines adopted following an EDPB binding decision are usually very significant. In the past years, the EDPB has transitioned from a body providing interpretations of legal texts to a decision-making authority weighing in on concrete cases.

To date, the EDPB has issued eleven binding decisions, with two of them being Art. 66 urgent binding decisions. In 2023, the EDPB adopted two Art. 65 binding decisions and one Art. 66 urgent binding decision, addressing a range of issues from privacy by design and by default, the principle of fairness, the processing of children's personal data, international transfers of data and the legal bases for behavioural advertising.

Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR)

In April 2023, the EDPB settled a dispute regarding a fine against Meta Platforms Ireland Limited (Meta IE), and an order to bring processing into compliance, in its **Binding Decision 1/2023**.

Following the EDPB's binding decision, Meta IE was issued a €1.2 billion fine by the Irish Data Protection Authority (Irish DPA). This fine was imposed for Meta's transfers of personal data to the U.S. on the basis of standard contractual clauses (SCCs) since 16 July 2020. Furthermore, Meta IE was ordered to bring its data transfers into compliance with the GDPR.

Andrea Jelinek, the EDPB Chair at the time, said: "The EDPB found that Meta IE's infringement is very serious since it concerns transfers that are systematic, repetitive and continuous. Facebook has millions of users in Europe, so the volume of personal data transferred is massive. The unprecedented fine is a strong signal to organisations that serious infringements have far-reaching consequences."

In its binding decision, the EDPB instructed the Irish DPA to amend its draft decision and to impose a fine on Meta IE. Given the seriousness of the infringement, the EDPB found that the starting point for calculation of the fine should be between 20% and 100% of the applicable legal maximum. The EDPB also instructed the Irish DPA to order Meta IE to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the U.S. of personal data of European users transferred in violation of the GDPR, within 6 months after notification of the Irish DPA's final decision.

The Irish DPA's final decision incorporates the legal assessment expressed by the EDPB in its binding decision, adopted on the basis of Art. 65(1)(a) GDPR after the Irish DPA, as lead supervisory authority (LSA), had triggered a dispute resolution procedure concerning the objections raised by several concerned supervisory authorities (CSAs). Among others, CSAs issued objections aiming to include an administrative fine and/or an additional order to bring processing into compliance.

Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)

In August 2023, the EDPB resolved a dispute on the draft decision of the Irish DPA on the processing of personal data of users between the ages of 13 and 17 by TikTok Technology Limited (TikTok IE). In its **Binding Decision 2/2023**, the EDPB analysed the design practices implemented by TikTok in the context of two pop-up notifications that were shown to children aged 13-17: the Registration Pop-Up and the Video Posting Pop-Up. The analysis found that both pop-ups failed to present options to the user in an objective and neutral way.

Following the EDPB's binding decision, the Irish DPA issued a final decision, finding, in particular, that TikTok IE infringed the GDPR's principle of fairness when processing personal data relating to children between the ages of 13 and 17 and imposed a reprimand, a compliance order and a fine of €345 million.

"Data protection authorities within the EDPB can effectively take action against big tech. The fine of 345 million euro imposed on TikTok led to better protection of all European children using this platform."

Aleid Wolfsen, Chair of the Dutch DPA and EDPB Deputy Chair

Anu Talus, EDPB Chair, said: "Social media companies have a responsibility to avoid presenting choices to users, especially children, in an unfair manner – particularly if that presentation can nudge people into making decisions that violate their privacy interests. Options related to privacy should be provided in an objective and neutral way, avoiding any kind of deceptive or manipulative language or design. With this decision, the EDPB once again makes it clear that digital players have to be extra careful and take all necessary measures to safeguard children's data protection rights."

In the Registration Pop-Up, children were nudged to opt for a public account by choosing the right-side button labelled "Skip", which would then have a cascading effect on the child's privacy on the platform, for example by making comments on video content created by children accessible.

In the Video Posting Pop-Up, children were nudged to click on "Post Now", presented in a bold, darker text located on the right side, rather than on the lighter button to "cancel". Users who wished to make their post private first needed to select "cancel" and then look for the privacy settings in order to switch to a "private account". Therefore, users were encouraged to opt for public-by-default settings, with TikTok IE making it harder for them to make choices that favoured the protection of their personal data. Furthermore, the consequences of the different options were unclear, particularly to child users. The EDPB confirmed that controllers should

not make it difficult for data subjects to adjust their privacy settings and limit the processing.

The EDPB also found that, as a result of the practices in question, TikTok IE infringed the principle of fairness under the GDPR. Consequently, the EDPB instructed the Irish DPA to include, in its final decision, a finding of this additional infringement and to order TikTok IE to comply with the GDPR by eliminating such design practices.

The EDPB also assessed whether age verification measures implemented by TikTok IE between 31 July and 31 December 2020 complied with the requirements of data protection by design (Art. 25(1) GDPR). The EDPB expressed serious doubts regarding the effectiveness of the age verification measures put in place by TikTok IE during this period, particularly taking into account the severity of the risks for the high number of children affected. Among others, the EDPB found that the age gate deployed by TikTok IE to prevent child users under the age of 13 from accessing the platform could be easily circumvented and that the measures applied after users gained access to TikTok IE were not applied in a sufficiently systematic manner.

The Irish DPA's final decision also includes legal assessment that was not subject to objections by CSAs, such as the finding that the public by default settings were contrary to the principles of data protection by design and default, of data minimisation and transparency.

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

Following the EDPB's **urgent Binding Decision 1/2023** of 27 October 2023, the Irish DPA adopted its final decision on 10 November 2023, imposing a ban on Meta IE for the processing of personal data for behavioural advertising purposes on the basis of contract and legitimate interest. The EDPB urgent binding decision followed a request from the Norwegian Data Protection Authority (NO DPA) to order final measures which would have effect in the entire European Economic Area (EEA).

EDPB Chair Anu Talus said: "After careful consideration, the EDPB considered it necessary to instruct the IE DPA to impose an EEA-wide processing ban, addressed to Meta IE. Already in December 2022, the EDPB Binding Decisions clarified that contract is not a suitable legal basis for the processing of personal data carried out by Meta for behavioural advertising. In addition, Meta has been found by the IE DPA to not have demonstrated compliance with the orders imposed at the end of last year. This has led to the use of the Art. 66 urgency procedure - a derogation from the usual cooperation procedure which can only be used in exceptional circumstances."

Initially, on 14 July 2023, the NO DPA adopted an order imposing a temporary ban under Art. 66(1) GDPR on Meta IE and Facebook Norway AS ("Facebook Norway") regarding the processing of personal data of Norwegian data subjects for

behavioural advertising relying on the legal bases of contract or legitimate interest. This ban was limited in time and geographic scope: it was valid for three months and only applicable in Norway. On 26 September 2023, the NO DPA submitted a request to the EDPB for an urgent binding decision to order the adoption of final measures applicable to users across the EEA.

Following its analysis of the file, the EDPB concluded that there were ongoing infringements of the GDPR and there was an urgent need to act in light of the risks for the rights and freedoms of the data subjects. In particular, based on the evidence provided, the EDPB found that there was an ongoing infringement of Art. 6(1) GDPR because of the inappropriate use of the legal bases of contract and legitimate interest for the processing of personal data collected by Meta IE for the purpose of behavioural advertising.

In addition, the EDPB concluded that there was also an ongoing infringement of Meta IE's duty to comply with decisions by DPAs, most notably the Irish DPAs final decisions of December 2022.

Regarding the existence of urgency, the EDPB concluded that the regular cooperation mechanisms could not be applied in their usual manner and that the urgent need to order final measures was clear in light of the risks of serious and irreparable harm caused to data subjects without the adoption of final measures.

Furthermore, the EDPB found that the Irish DPA failed to address a request for mutual assistance from the NO DPA within the timeframe set out in the GDPR. The presumption of urgency set by Art. 61(8) GDPR thus applied, which further corroborated the need to derogate from the regular cooperation and consistency mechanisms.

Consequently, the EDPB decided that final measures needed to be adopted by the Irish DPA. It considered appropriate, proportionate and necessary to instruct the Irish DPA to impose a ban on processing addressed to Meta IE for processing of personal data collected on Meta IE's products for behavioural advertising purposes on the basis of contract and legitimate interest.

This urgent binding decision was addressed to the Irish DPA, the NO DPA and the other concerned DPAs, and the Irish DPA adopted its final decision on 10 November 2023.

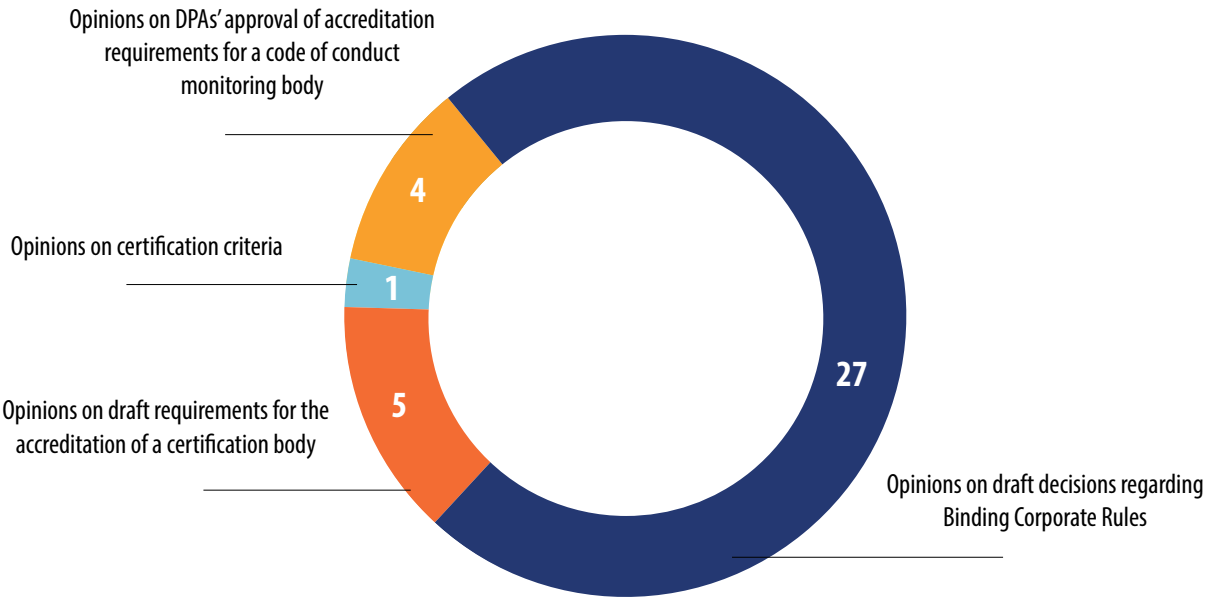
2.2. CONSISTENCY OPINIONS

The Board issues consistency opinions to contribute to the consistent application of the GDPR. DPAs may seek consistency opinions from the EDPB under Art. 64(1) GDPR when they intend to adopt certain types of measures. Following a consistency opinion, DPAs adopt their national decisions.

The EDPB can adopt six different types of opinions on DPAs' draft decisions: (a) when they aim to adopt a list of processing operations subject to the requirement for a data protection impact assessment, (b) concerning a draft code of conduct, (c) when they aim to approve the requirements for the accreditation of a certification body or the criteria for certification, (d) when they aim to determine standard contractual clauses, (e) when they aim to authorise standard contractual clauses and (f) when they aim to approve Binding Corporate Rules (BCRs). In 2023, the EDPB adopted a total of 37 consistency opinions (Art. 64(1)). *See Section 4.4. for the complete list of opinions adopted in 2023.*

Since 2018, the EDPB has adopted 182 consistency opinions in total. This way, starting from a theoretical description of new compliance tools introduced in the GDPR, the EDPB has built a framework for the new compliance tools, such as codes of conduct and certification mechanisms, to become operational in a consistent manner.

Consistency opinions in 2023



The EDPB has made significant progress in the area of certification as a compliance tool (Art. 42 GDPR) and as a tool for transfers (Art. 46(2)(f) GDPR). In addition to the final version of Guidelines 07/2022 on certification as a tool for transfers and the EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals, both adopted at the beginning of 2023, EDPB members also held two certification workshops in Spring and Autumn 2023. The workshops took place in Spain and Luxembourg, respectively, and the aim was to find synergies, strengthen cooperation among EDPB members on this topic and address the main challenges and opportunities that these tools present. During the first day of the Autumn workshop, certification stakeholders had the opportunity to provide feedback and share their experiences. The EDPB continues to work on the topic of certification, including certification as a tool for transfers, which confirms its commitment, as reflected in the 2021-2023 Strategy, to advance harmonisation and facilitate the implementation of compliance mechanisms.

2.3. GENERAL GUIDANCE

One of the EDPB's core competences is to clarify the GDPR by issuing guidance. During the initial phase of the GDPR's implementation, the EDPB established a well-defined and comprehensive repository of guidelines and recommendations. This ensures that DPAs apply data protection laws consistently and it further strengthens stakeholder compliance. The EDPB continues to build and expand its guidance and makes a consistent effort to incorporate stakeholder input, which is collected via public consultation.

"One of the things we have worked on together at European level is a more targeted guidance effort. We explain the rules shorter, clearer and more user-oriented."

Cristina Angela Gulisano,
Director of the Danish DPA

In 2023, the EDPB adopted two new guidelines, as well as nine guidelines and one set of recommendations following public consultation.

See Section 4.2. for the complete list of guidelines and recommendations.

Based on the interest shown by stakeholders during the public consultation phase in Guidelines 03/2022 and 05/2022, the following sub-chapters will elaborate on each one respectively.

2.3.1. Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them

The EDPB adopted Guidelines 03/2022 after public consultation, on 14 February 2023. Their aim is to lay down practical recommendations and guidance to social media providers as controllers of social media, designers and users of social media platforms, on how to assess and avoid deceptive design patterns in social media interfaces. The existence of such patterns often lead users to make unintended, unwilling, and/or potentially harmful decisions concerning the processing of their personal data.

The guidelines provide a non-exhaustive list of deceptive design patterns during the life cycle of a social media account (i.e. from the sign-up stage to the closing of a social media account) as well as elaborate on the best practices at the end of each use case. The types of dark patterns addressed in the guidelines are the following:

(a) overloading: when users are confronted with a large quantity of information, options or possibilities in order to be prompted to share more data or unintentionally allow the processing of their personal data against their expectations.

(b) skipping: when the design of the interface or users' journey is made in a way that users forget or do not think about all or some of the data protection aspects.

(c) stirring: when the choice of the users is affected by appealing to their emotions or using visual nudges.

(d) obstructing: when the users are hindered or blocked in their process of becoming informed or managing their data by making such action hard or impossible to achieve.

(e) fickle: when the design of the interface is not consistent and clear, making it hard for the users to navigate the different data protection control tools and to understand the purpose of the processing.

(f) left in the dark: when the interface is designed to hide information or data protection controls or to leave users unsure of how their data are processed and what kind of control they might have over it regarding the exercise of their rights.

The guidelines provide concrete examples on deceptive design patterns and on recommended best practices. For example, with respect to the deceptive design of "obstructing", where users are not provided with any links to data protection information once they have started the sign-up process, users cannot find this information as none is provided anywhere in the sign-up interface, not even in the footer. To avoid this, the guidelines provide some best practices, such as the use of shortcuts.

The EDPB recalls the obligations of social media providers under GDPR and particularly recommends the use of interdisciplinary teams, including designers, data protection officers and decision-makers to ensure GDPR compliance on their platforms.

The recommendations set forth in the guidelines can be used from the early conception phase of a user interface to avoid the implementation of deceptive design patterns, as well as on an existing service to evaluate the interface's compliance with GDPR requirements.

2.3.2. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

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

FRT relies on the processing of biometric data, which benefit from special protection in the data protection legal framework. Indeed, biometric data are permanently and irrevocably linked to an individual's identity. The sheer size of processing of personal data, and in particular biometric data, is a further key element of FRT, as the processing of personal data constitutes an interference with the fundamental right to protection of personal data according to Art. 8 of the Charter of Fundamental Rights of the European Union (the Charter).

The use of FRT by LEAs will have – and to some extent already does have – significant implications on individuals and on groups of people, including minorities. These implications will also have considerable effects on the way we live together and on our social and democratic political stability. The application of FRT is considerably prone to interfere with fundamental rights beyond the right to protection of personal data.

"Technology took a giant leap over the past decades and regulators are faced with new, increasingly complex technological and social scenarios."

Pasquale Stanzione,
President of the Italian DPA

With its Guidelines, the EDPB deems it important to contribute to the ongoing integration of FRT in the area of law enforcement covered by the Law Enforcement Directive and the national laws transposing it. The guidelines provide relevant information to lawmakers at EU and national level, as well as for LEAs and their officers when implementing and using FRT-systems. The scope of the guidelines is limited to FRT. However, other forms of processing of personal data based on biometrics by LEAs, especially if processed remotely, may entail similar or additional risks for individuals, groups and society. The guidelines provide information on certain properties of FRT and outline the applicable legal framework in the context of law enforcement that lawmakers at national and EU level, as well as LEAs using the FRT systems, must strictly comply with to ensure the protection of data subjects' rights.

The guidelines also provide a tool to support a first classification of the sensitivity of a given use case (Annex I), as well as practical guidance for LEAs that wish to procure and run a FRT-system (Annex II). Furthermore, the guidelines also depict several typical use cases and list relevant considerations, especially with regard to the necessity and proportionality test (Annex III).

"For the national data protection authority, the most significant challenge for the future is striking a balance between the rights of data subjects, obligations of data controllers and rapidly developing technologies."

Jekaterina Macuka,
Director of the Latvian Data State Inspectorate

2.4. LEGISLATIVE CONSULTATION

In the context of legislative consultations requested by the European Commission, the EDPB adopts opinions on issues pertaining to data protection in the EU. Opinions may be adopted solely by the EDPB or jointly with the EDPS. The EDPB may also advise the Commission on the assessment of the adequacy of the level of protection in a third country.

A noteworthy output of the EDPB's efforts in 2023 is its Joint Opinion 01/2023 with the EDPS on the Proposal for a Regulation laying down additional procedural rules relating to the enforcement of Regulation (EU)2016/679. This legislative initiative follows the EDPB's 2022 wish list.

Regarding cooperation with third countries, the EDPB provided its Opinion 5/2023 in February 2023 on the European Commission's Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. Adequacy decisions, which are negotiated by the European Commission, are a key instrument of the GDPR for data transfers, and require the EDPB's consultation.

Based on the high strategic relevance and strong stakeholder impact, the following sub-chapters will elaborate on Joint Opinion 01/2023 and Opinion 05/2023.

2.4.1. Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework

On 28 February 2023, the EDPB adopted Opinion 5/2023 in relation to the Commission's draft adequacy decision regarding the framework for transatlantic exchanges of personal data, referred to as "the EU-US Data Privacy Framework" (DPF). With its Opinion, the EDPB provides input to the Commission regarding the adequacy of the level of protection afforded to individuals whose personal data is transferred to the U.S. through the Draft Decision, which considers both the commercial aspects and U.S. public authorities' access and use of data. The key component of the DPF is the EU-US Data Privacy Framework Principles, which were issued by the U.S. Department of Commerce.

The EDPB welcomes substantial improvements such as the introduction of requirements embodying the principles of necessity and proportionality for U.S. intelligence gathering of data and the new redress mechanism for EU data subjects. At the same time, it expresses concerns and requested clarifications on several points. These related, in particular, to certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the practical functioning of the redress mechanism. The EDPB notes it would welcome that not only the entry into force but also the adoption of the decision are conditional upon the adoption of updated policies and procedures to implement Executive Order (EO) 14086 by all U.S. intelligence agencies. The EDPB recommends the Commission to assess these updated policies and procedures and share its assessment with the EDPB.

Regarding commercial aspects, the EDPB welcomes a number of updates made to the DPF Principles. Notably, a number of Principles remain essentially the same as under the Privacy Shield. Thereby, the EDPB underlines some of its previous concerns, for example, relating to some exemptions to the right of access, the absence of key definitions, the lack of clarity about the application of the DPF Principles to processors, the broad exemption to the right of access for publicly available information, and the lack of specific rules on automated decision-making and profiling. The EDPB further reiterates that the level of protection must not be undermined by onward transfers. Therefore, it invites the Commission to clarify that the safeguards imposed by the initial recipient on the importer in the third country must be effective in light of third country legislation, prior to an onward transfer. Moreover, the EDPB asks the Commission to clarify the scope of the exemptions regarding the duty to adhere to the DPF Principles and stressed the importance of effective oversight and enforcement of the DPF. These aspects will be closely monitored by the EDPB, together with the effectiveness of the redress avenues provided to EU data subjects whose data are processed in violation of the DPF.

Regarding government access to data transferred to the U.S., the EDPB acknowledges the significant improvements brought by EO 14086. The EO introduces the concepts of necessity and proportionality with regard to U.S. intelligence-gathering of data (signals intelligence). Furthermore, the new redress mechanism creates rights for EU individuals and is subject to the review by the Privacy and Civil Liberties Oversight Board (PCLOB). The EO also enshrines more safeguards to ensure the independence of the Data Protection Review Court (DPRC), compared to the previous Ombudsperson mechanism, and introduces more effective powers to remedy violations, including additional safeguards for data subjects.

The EDPB highlights that close monitoring is needed concerning the practical application of the newly introduced principles of necessity and proportionality. Further clarity is also necessary regarding temporary bulk collection and the further retention and dissemination of the data collected in bulk. The EDPB also expresses concerns about the lack of a requirement of prior authorisation by an independent authority for the collection of data in bulk under EO 12333, as well as the lack of systematic independent review *ex post* by a court or an equivalently independent body. With regard to prior independent authorisation of surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA), the EDPB regrets that the FISA Court does not review compliance with EO 14086 when certifying programmes authorising the targeting of non-U.S. persons, even though the intelligence authorities carrying out the programme are bound by it. Reports of the PCLOB on how the safeguards of the EO 14086 will be implemented and how these safeguards are applied when data is collected under Section 702 FISA and EO 12333 would be particularly useful. Regarding the redress mechanism, the EDPB recognises the additional safeguards provided, such as the role of the special advocates and the review of the redress mechanism by the PCLOB. At the same time, the EDPB is concerned about the general application of the standard reply of the DPRC notifying the complainant that either no covered violations were identified or a determination requiring appropriate remediation was issued, especially given that this decision cannot be appealed. The EDPB therefore calls on the Commission to closely monitor the practical functioning of this mechanism.

Following the EDPB opinion, on 10 July 2023, the European Commission adopted its Implementing Decision C(2023) 4745 on the adequate level of protection of personal data under the EU-US Data Privacy Framework (DPF Adequacy Decision).[7] By doing so, the Commission decides that the U.S., for the purpose of Art. 45 GDPR, ensures an adequate level of protection for personal data transferred from the EU to organisations in the U.S. that are included in the "Data Privacy Framework List", maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I of the DPF Adequacy Decision.

Moreover, the DPF Adequacy Decision entrusts the EDPB Secretariat as the single point of contact at EU level for routing complaints of individuals alleging unlawful access by US intelligence agencies from the EU/EEA DPAs to the Civil Liberties Protection Officer in the Office of the Director of National Intelligence.

On September 2023, the EDPB adopted an Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023. This info note provides some clarity on the implications of the DPF Adequacy Decision for data subjects in the EU and for entities transferring personal data from the EU to the U.S. It includes information on the practical consequences of the adoption of the DPF Adequacy Decision, both with regard to transfers to the U.S. under the DPF as well as transfers on the basis of other transfer tools. The Info note also provides information on how data subjects in the EU can lodge complaints under the DPF, both for commercial aspects, as well as for national security purposes, as well as the date of the review of the adequacy decision.

[7] Implementing Decision C(2023) 4745 of the European Commission, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ('GDPR') on the adequate level of protection of personal data under the EU-US Data Privacy Framework ('the Adequacy Decision') of 10 July 2023.

2.4.2. EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679

On 4 July 2023, the Commission published a Proposal for a Regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 ("the Proposal"). The EDPB and EDPS were formally consulted and issued Joint Opinion 01/2023 on 19 September 2023.

In their Joint Opinion, the EDPB and EDPS welcome many of the improvements introduced by the Proposal, especially those aimed at building consensus between the DPAs "by design" and at ensuring that complaints are dealt with more effectively. In addition, the EDPB and EPDS positively note the Proposal's objective to further harmonise the procedural rights of the parties under investigation and the complainants.

"We as supervisory authorities must work towards greater speed and commitment in case processing in order to effectively enforce the GDPR. We need to ensure that the fundamental rights of citizens are respected."

Ulrich Kelber,
the German Federal Commissioner for Data Protection and Freedom of Information

However, the EDPB and EDPS also raise some concerns and make a number of recommendations in order to ensure that the new Regulation will work in practice and that the DPAs will be able to investigate and deliver results for individuals more rapidly.

The Joint Opinion highlights, among others, that the EDPB's current approach used for the preparation of EDPB binding decisions should not be changed. More specifically, the requirement to provide the parties under investigation and the complainant with a "statement of reasons" should be removed as it is not in line with the specific architecture of the OSS mechanism. The current practice whereby the parties provide their views prior to the matter being referred to the EDPB on all elements relied upon for the decision should be kept as it allows the EDPB to duly take such views into account and adopt a decision within the legal deadlines.

Next, the EDPB and EDPS welcome the new requirement for the LSA to share a "summary of key issues" with the CSAs early in the procedure since it fosters enhanced cooperation. However, the content and meaning of the summary of key issues need to be further clarified. In addition, the LSA's "preliminary findings" and "preliminary view" must be shared with the CSAs for comment, before they are shared with the parties under investigation and the complainant, and the LSA should be obliged to engage with the CSAs in an attempt to find a consensus at the earliest stage possible.

Further, the EDPB and EDPS are concerned that the Proposal unduly redefines and restricts the CSAs' ability to raise relevant and reasoned objections on a draft decision, including on the scope of the investigation, and recommend removing this restriction form the final text of the new Regulation.

Finally, the EDPB and EDPS take the view that the Proposal unduly restricts the application of the urgency procedure by limiting the territorial scope of the adopted final measures to the territory of the Member State of the DPA requesting the urgent opinion or decision. Such a change would lead to a multiplication of requests to the EDPB and to a fragmentation of final measures. Therefore, considering that the urgency procedure applies *per se* to cross-border processing and that its purpose is to address exceptional circumstances by providing harmonised solutions, the urgent decision or opinion should be addressed to all CSAs and be binding on them.

2.5. STAKEHOLDER CONSULTATION

2.5.1. Public consultation

Following the preliminary adoption of guidelines, the EDPB organises public consultations to give stakeholders and citizens the opportunity to provide additional input. The EDPB considers this input before adopting the guidelines in their final version. Feedback on the value of the guidance and general work of the EDPB is appreciated as it provides useful insights into the needs of stakeholders. To increase transparency, the stakeholders' contributions to public consultations are published by the EDPB on its website. In 2023, two public consultations were launched on Guidelines 01/2023 and 02/2023.

2.5.2. Survey on practical application of adopted guidance

In 2023, the EDPB conducted the sixth annual survey to review its activities under Art. 71(2) GDPR. The survey focused on the EDPB's work and output during the year, particularly its guidelines, joint opinions, and consultation work. It was conducted with a view to determine the usefulness of its guidance for interpreting GDPR provisions and identify areas in which better support could be provided to organisations and individuals in navigating the EU data protection framework.

Among the key stakeholders surveyed were academics in the field of data protection and privacy rights, business and legal professionals, and members of non-governmental organisations.

In general, the stakeholders surveyed noted that the EDPB's guidelines offer high practical value by providing context to complex regulations in a comprehensive manner. Regarding Guidelines 2/23 on Technical Scope of Art. 5(3) of ePrivacy Directive, stakeholders highlighted their accessibility, alongside their useful and actionable information.

Stakeholders highlighted their continual reliance on a wide range of guidelines and recommendations prior to 2023. Praise was notably given to Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement as well as those guidelines released by the EDPB which formed part of the Work Programme 2023-2024. This includes Guidelines 01/2022 on data subject rights - Right of access, Guidelines 9/2022 on personal data breach notification under GDPR and Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority.

The stakeholders indicated that the guidelines provide well-illustrated examples that are understandable and enable easy application, even where the stakeholders' primary field is not data protection. A limited number of stakeholders, however, deemed the language somewhat too technical and specific for the larger public, despite the accessibility to a wide range of professionals. At the same time, they found them well-written for their main audiences – professionals in the data protection world. To further improve the guidelines,

visualisations such as videos were recommended that can provide higher clarity on more technical sections of the guidelines. Stakeholders also observe that although the examples in the guidelines are useful and helpful, it would be useful if more examples were included.

The surveyed stakeholders confirmed that they consulted the EDPB's guidelines and joint opinions on a near-daily basis for professional purposes in 2023 and generally accessed them directly through the EDPB website or search engines. They indicated that they primarily relied on EDPB's guidance to expand their knowledge and support legal analysis in areas where case law is still unclear. In these circumstances, the EDPB guidelines are a valuable resource of information, which can be easily referenced and applied to professional contexts.

As a whole, the EDPB's guidelines were noted as being easy to consult by the stakeholders, with positive reference made to both the structure and layout of the document. The summaries presented within the guidelines were highlighted as an important and appreciated inclusion, although a suggestion was made to shorten these overviews where possible, to prioritise conciseness and avoid repetition. Additionally, adding an executive summary as a standard section of every document would increase the ease of use of the guidelines. Although the EDPB guidelines are frequently lengthy, stakeholders highlighted it as being necessary to promote a common understanding of EU data protection laws. Translations of the guidelines also prove useful for their interpretation before other intuitions and improve ease of use for stakeholders. Whilst references to external citations are not featured within the guidelines, a stakeholder noted that the inclusion of such academic work may provide additional context and resources for those who wish to gain more knowledge on the area at hand.

With respect to the public consultations organised by the EDPB, significant praise and appreciation were noted for the frequency of these opportunities to contribute either as a team or as an individual. The stakeholders who actively engaged in public consultations noted that their involvement was a positive experience; this also extended to those who participated in the Pool of Experts consulted by the EDPB.

In relation to the EDPB's future work, stakeholders look forward to the continuation of the EDPB's interpretation of the GDPR and subsequent binding decisions, and express their eagerness to receive further helpful guidance, particularly on the topic of anonymisation.

The EDPB highly values the engagement and input from its stakeholders. The feedback on the significance of the guidance and general work of the EDPB provides useful insights into the needs of stakeholders, that will be considered by the EDPB.

2.6. REPRESENTING THE EDPB WORLDWIDE

One of the EDPB's strategic objectives (EDPB Strategy 2021-2023) is to engage with the international community to promote EU data protection as a global model and to ensure effective protection of personal data beyond EU borders. To this end, the EDPB launched the task force on international engagement and took part in international fora such as the Global Privacy Assembly, the Spring Conference and the G7's DPA Roundtable.

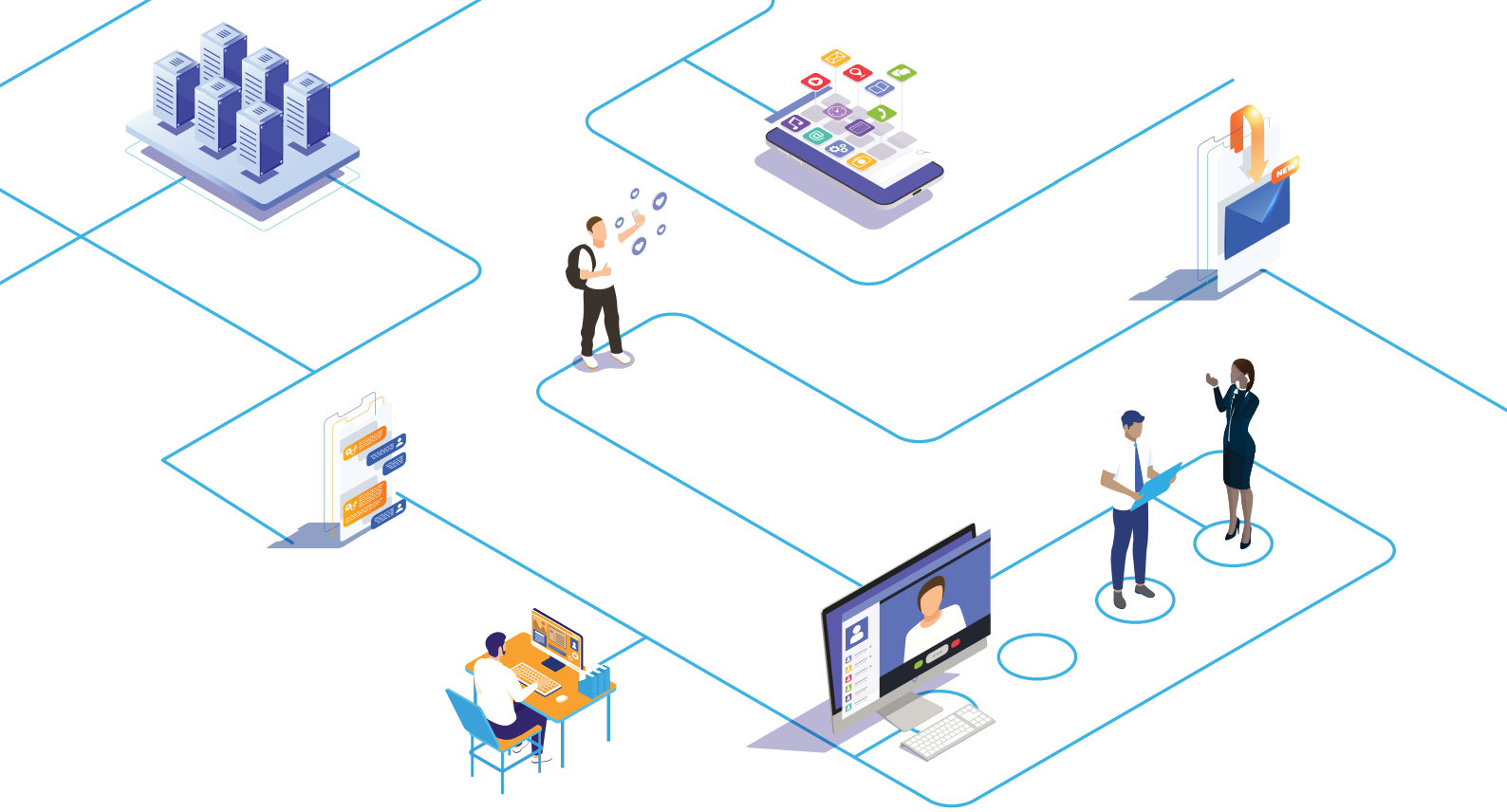
In addition, in 2023, the EDPB Chairs took part as a keynote speaker in the IAPP Global Privacy Summit and the Privacy Symposium in April; the Global Privacy Assembly in October and the IAPP Europe Data Protection Congress in November.

"In these 5 years the EDPB has strengthened the bonds among its members. In the next 5 years, hopefully it will broaden its relations with authorities and stakeholders outside the EU, as its works have a global impact for improving people's lives worldwide."

Irene Loizidou Nicolaidou,
Cypriot Commissioner for Personal Data Protection and EDPB Deputy Chair

In total, the Chairmanship of the EDPB had over 28 speaking engagements in 2023. As former EDPB Chair, Dr Andrea Jelinek had 8 speaking engagements, before being replaced by Dr Anu Talus as new EDPB Chair in May 2023, who spoke at 17 events in 2023. Deputy Chairs Irene Loizidou Nicolaidou, who was elected in May 2023, and Aleid Wolfsen, alongside outgoing Deputy Chair Ventsislav Karadjov, took part in 3 speaking engagements. These speaking engagements included press briefings, presentations, and panel discussions for a range of institutes, academic forums, and policy agencies.

A total of 40 speaking events were attended both in person and remotely by the EDPB staff. These events were largely hosted by, amongst others, universities, law firms, companies and EU institutions.



3. ENFORCEMENT COOPERATION AND ENFORCEMENT BY DPAs

3.1. EDPB ACTIVITIES TO SUPPORT GDPR ENFORCEMENT AND COOPERATION AMONG DPAs

Coordinated Enforcement Framework

The importance of consistent enforcement through cooperation efforts has been emphasised by the EDPB ever since the adoption of the GDPR. In 2020, the EDPB set up a Coordinated Enforcement Framework (CEF), with the aim of streamlining enforcement and cooperation among DPAs, in line with its 2021-2023 Strategy. The CEF consists of annual joint actions on a specific topic, including activities such as joint awareness campaigns, information gathering, enforcement sweeps as well as joint investigations. These annual coordinated enforcement efforts are intended to improve compliance, empower individuals to exercise their rights and increase awareness of data protection issues.

For its 2023 Coordinated Enforcement Action, the EDPB selected "the Designation and Position of Data Protection Officers". Throughout 2023, 25 DPAs across the EEA conducted coordinated investigations. Various organisations, as well as individual DPOs were contacted across the EEA, covering a wide range of sectors (both public and private entities), and more than 17,000 replies were received and analysed. Extensive data was collected offering valuable insights into the profile, position and work of DPOs 5 years after the entry into application of the GDPR. The DPAs consolidated their findings into national reports, which were then combined to produce an EDPB report, listing the obstacles currently faced by DPOs, along with a series of recommendations to further strengthen their role. Among others, the report encourages DPAs to carry out more awareness-raising activities, information and enforcement actions. The report also encourages organisations to ensure that DPOs have sufficient

opportunities, time and resources to refresh their knowledge and learn about the latest developments.

Support Pool of Experts

The Support Pool of Experts (SPE) is a key initiative of the EDPB within its 2021-2023 Strategy, which helps DPAs increase their capacity to supervise and enforce the safeguarding of personal data. The SPE provides support in the form of expertise for investigations and enforcement activities of common interest to DPAs and enhances cooperation by reinforcing and complementing the strengths of the individual DPAs and addressing operational needs. This includes but is not limited to, analytical support, assistance in the performance findings of a forensic nature, as well as in the preparation of investigative reports on the basis of evidence collected.

To better coordinate the work of the SPE, the EDPB set up a list of SPE contact points within the DPAs, at the end of 2021. In addition, the EDPB launched a call for expressions of interest "Establishment of a List of Individual Experts for the implementation of the EDPB's Support Pool of Experts" in February 2022. The objective of this call is to set up a reserve list of external experts with legal or technical expertise. At the end of 2023, the EDPB counted around 500 experts on its reserve list. These experts are qualified in areas such as IT auditing, website security, mobile OS and apps, IoT, cloud-computing, behavioural advertising, anonymization techniques, cryptology, AI, UX design, fintech, data science, digital law, etc. They may assist DPAs in different stages of their investigation and enforcement activities in the field of data protection. So far, a total of 13 projects, some of which are on AI-related matters, have been launched since July 2022.

Lastly, in June 2023, the EDPB organised a boot camp on website inspections, where it invited several DPA experts. This event was a great occasion to use and discuss the new EDPB website auditing tool developed in the framework of the SPE, and which is now published as open source code on code.europa.eu. A second boot camp will be organised in 2024.

"An important challenge for data protection authorities is the accelerated growth of new technologies based, among others, on artificial intelligence, blockchain, ubiquitous computing and connected objects, quantum computing, virtual reality and augmented reality. The completely innovative and disruptive use cases that emerge there very often raise questions about the protection of personal data and users' privacy. DPAs must accelerate acquisition of new expertise in these domains and intensify collaboration between themselves and with other regulators."

Tine A. Larsen,
Chair of the Luxembourg's DPA

Taskforces

A number of taskforces have worked on key topics with a cross-border dimension in 2023, in order to ensure a consistent approach by the DPAs. Two reports on the work undertaken by taskforces were adopted in 2023, namely the Report of the Cookie Banner Taskforce and the Report of 101 Taskforce.

The Cookie Banner Taskforce was created to examine and provide a coordinated response to the "cookies banner" complaints received by None of Your Business (NOYB). This taskforce was established in accordance with Art. 70(1)(u) GDPR to promote cooperation, information sharing and best practices between DPAs, specifically regarding the use by controllers of cookies banners. The Report of the work undertaken by the Cookie Banner Taskforce includes the common denominator between DPAs in their interpretation of the applicable provisions of the ePrivacy Directive and of the GDPR, on issues such as reject buttons, pre-ticked boxes, banner design, or withdraw icons. Throughout 2023, the Taskforce members continued to share updates on the handling of NOYB complaints and discuss their findings and analyses. The Report of the work undertaken by the Cookie Banner Taskforce examines eight different practices implemented by websites and that were the subject of the complaints received. These include the absence of a "reject" button on the first layer of the cookie banner, the use of pre-ticked boxes for consent to cookies, banner design, or the absence of an icon to withdraw consent. The Report includes the common denominator between DPAs in their interpretation of the applicable provisions of the ePrivacy Directive and of the GDPR on these eight practices. For example, DPAs were of the view that even though website owners should implement easily accessible solutions to allow users to withdraw their consent, they cannot be imposed a specific withdrawal solution. Throughout 2023, the Taskforce members continued to share updates on the handling of NOYB complaints and discuss their findings and analyses.

The 101 Taskforce was created to handle the "101 complaints" received from NOYB regarding transfers of personal data. The complaints particularly revolved around the implementation of the tools "Google Analytics" and "Facebook Business Tools" on a website. The Report of the work undertaken by the DPAs within the 101 Taskforce provides a complete assessment of the complaints, focusing namely on the transfers of personal data, the principle of accountability and the allocation of roles between the website and the provider of the two tools. More specifically, the Report reflects the common denominator agreed by the DPAs in their interpretation of the applicable provisions of the GDPR. For example, the Report highlights that in cases where website operators are regarded as data controllers, they must carefully examine whether the respective tool can be used in compliance with data protection requirements in accordance with the principle of accountability. The DPAs' common assessment has enabled several DPAs to adopt consistent decisions, such as ordering website operators to comply with the transfer provisions of the GDPR, and if necessary, to stop the data transfer at stake.

The EDPB also decided to launch another taskforce in 2023 in light of the recent enforcement action undertaken by the Italian data protection authority against Open AI about the Chat GPT service.

EDPB Template Complaint Form

The EDPB Template Complaint Form was adopted in June 2023 in order to facilitate the submission of complaints by individuals regarding possible infringements in connection with the processing of their personal data. The Template Complaint Form also aims at facilitating the subsequent exchange of information between DPAs and at ensuring a more efficient handling of such complaints by the DPAs.

In its Joint Opinion 01/2023, the EDPB and EDPS welcomed significant similarities between the Commission's proposal to harmonise the information to be provided for a complaint to be admissible and

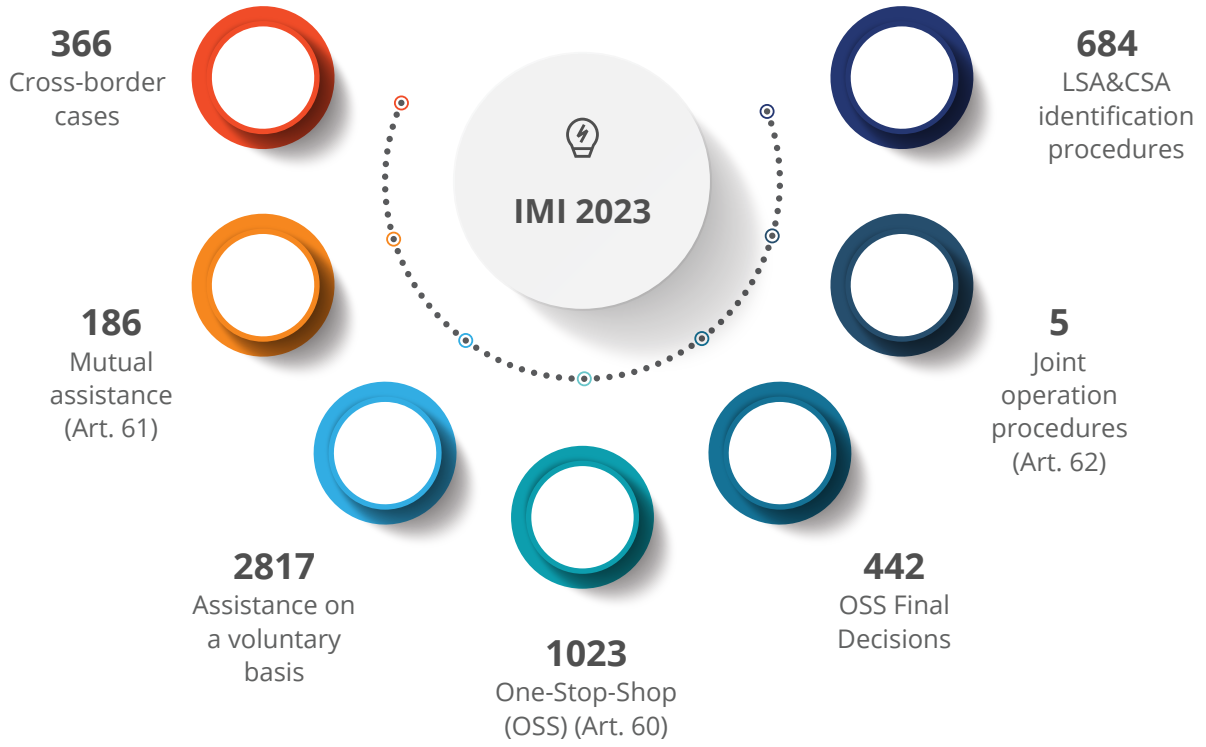
the EDPB Template Complaint Form. It is the opinion of the EDPB and EDPS that "complaints constitute a cornerstone of the supervisory work for enforcing the GDPR" and the right to file a complaint should not be restricted by imposing unnecessary administrative burdens on those filing complaints.

3.2. COOPERATION UNDER THE GDPR

Under the GDPR, national Data Protection Authorities (DPAs) have a duty to cooperate to ensure the consistent application of data protection law.

In cases that have a cross-border component, the DPAs have a range of tools at their disposal, such as the mutual assistance, joint operations and the One-Stop-Shop cooperation mechanism to facilitate harmonisation.

A case with a cross-border component is registered in a central database via the IMI. In total, 366 cross-border cases have been created in the EDPB's case register, and 1023 procedures related to the One-Stop-Shop (Art. 60 GDPR) have been triggered in 2023, out of which 442 Final Decisions.



Please note that:

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

3.3. CASE DIGEST

Case digest on security of processing and data breach notification

For the second time,[8] the EDPB commissioned a thematic case digest as part of its SPE initiative. Case digests are overviews of decisions adopted under the one-stop-shop procedure about a particular topic. The purpose of these digests is to give the DPAs and the general public, including privacy professionals, insight into the decisions adopted by DPAs following cross-border cooperation procedures.

Professor Eleni Kosta[9] drafted a case digest based on 90 decisions for which DPAs cooperated with one another under the OSS mechanism in the field of security of data processing and data breach notifications.[10] More specifically, these decisions relate to Art. 32 GDPR (security of processing), Art. 33 GDPR (notification of a personal data breach to the DPA) and Art. 34 GDPR (communication of a personal data breach to the data subject). All of these decisions were adopted between January 2019 and June 2023. The case digest also refers to the available guidance at EU level, and in particular, EDPB Guidelines 9/2022 on personal data breach notification under GDPR and Guidelines 01/2021 on examples regarding personal data breach notification. Relevant cases before the Court of Justice of the EU, as well as decisions and guidance adopted at national level are mentioned, such as national guidance on the use of robust passwords and secure authentication channels.

DPAs often applied Arts. 32, 33 and 34 GDPR altogether in their decisions, given that the occurrence of a data breach is in most cases linked to the implementation of security measures. Many decisions relate to data breaches caused by malicious attacks by third-party hackers, insufficient internal practices and IT systems or human error. As a result, the case digest offers insights on the interpretation and application of these GDPR provisions by DPAs in all of these diverse scenarios.

Art. 32 GDPR sets out an obligation for both data controllers and data processors to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk". In that regard, the case digest constitutes a valuable resource, analysing how DPAs assessed whether the security measures implemented by organisations were appropriate. More specifically, DPAs carried out analyses of the technical and organisational measures implemented - both before the occurrence of a data breach (through preventive measures) and after such occurrence (through remedial or mitigating measures). Despite the fact that the DPAs analysed the relevant security measures on a case-by-case basis taking into account the specifics of the affected data processing, conclusions can still be drawn regarding whether certain security measures are considered sufficient by DPAs. For instance, several DPAs examined the establishment of proper access control mechanisms based on the individual authentication to access specific data. Lack of such clear access control mechanisms led various DPAs to find violations of

[8] Case digest on the right to object and the right to erasure, Alessandro Mantelero, 9 December 2022, https://edpb.europa.eu/system/files/2023-02/one-stop-shop_case_digest_on_the_right_to_object_and_right_to_erasure_en.pdf.

[9] Professor of Technology Law and Human Rights, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.

[10] The EDPB's public register with the one-stop-shop final decisions is available at https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en. Annex 1 to the case digest lists the decisions relied upon and provides the link to the redacted decisions, which are available on the EDPB's public register.

Art. 32 GDPR. Other decisions show similarities in the conclusions reached by DPAs, for example regarding the storage and encryption of passwords, and the recording of logs.

Under Art. 33 GDPR, data controllers are required to notify the competent DPA of a personal data breach "without undue delay" and – "where feasible" – "not later than 72 hours after having become aware of it". A notification to the DPA is not mandatory when the personal data breach is unlikely to result in a "risk to the rights and freedoms of natural persons". The analysis of the OSS decisions sheds some light on how data controllers should document their compliance with this provision.

Lastly, Art. 34 GDPR establishes an obligation for data controllers to communicate the personal data breach to the affected individuals "without undue delay", when the personal data breach is likely to result in a "high risk to the rights and freedoms of natural persons".

This case digest analyses the findings of DPAs in very diverse scenarios, such as in the event of ransomware, compromised hardware or accounts and accidental disclosures of personal data. It creates a rich pool of analyses of different security incidents, along with the corresponding security measures that DPAs found to be appropriate or not in the specific context. As a result, the case digest constitutes a very useful tool for DPAs and their case officers when assessing similar cases in the future. The decisions mentioned also enable organisations to grasp which preventive security measures they may choose to implement when processing personal data, and/or which remedial measures to adopt following a personal data breach. All the decisions referred to in the case digest are easily accessible with a direct link to the EDPB's public register.

3.4. NATIONAL CASES WITH EXERCISE OF CORRECTIVE POWERS

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

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

In 2023, DPAs issued a number of fines, as indicated in the table on the following page.

DPA	Number of fines	Total Fines amount
Austria	55	€254 075
Belgium	3	€80 000
Bulgaria	93	€159 931
Croatia	28	€8 266 350
Cyprus	11	€120 250
Czech Republic	23	€140 000
Denmark	5	€2 100 000
Estonia	12	€213 300
Finland	3	€464 600
France	37	€79 164 500
Germany (all Länder grouped together)	469	€9 743 930
Greece	12	€636 000
Hungary	95	€1 380 334
Iceland	12	€537 000
Ireland	6	€1 551 782 500
Italy	146	€25 200 000
Latvia	3	€22 900
Liechtenstein	1	€500
Lithuania	13	€64 060
Luxembourg	3	€6 500

DPA	Number of fines	Total Fines amount
Malta	3	€32 500
Netherlands	8	€ 243 160 000
Norway	7	€8 500 000
Poland	24	€213 820
Portugal	48	€367 450
Romania	68	€444 622
Slovakia	47	€122 665
Slovenia	77	€56 910
Spain	367	€29 817 410
Sweden	11	€10 780 000
		€1 973 832 107

The EDPB website includes a selection of DPA supervisory actions. This section of the Annual Report contains a non-exhaustive list of certain national enforcement actions in different EEA countries. Some of the cases presented in this section were dealt with through the OSS cooperation mechanism.

Some cases examined in this section highlighted a lack of proper technical and organisational measures for processing personal data securely. Many cases revolved around the lack of a legal basis including data processing without individual's consent. In some instances, DPAs dealt with cases involving the unlawful processing of special categories of personal data, such as health data. A great number of cases also included the failure of data controllers to provide information about their processing activities and the violation of individual rights, such as the right to erasure and the right of access. Moreover, some significant incidents involved the failure to notify individuals of the occurred or the potential risk of data breaches. Both private and public entities were imposed fines by the national DPAs.

3.4.1. AUSTRIA

In 2023, the Austrian DPA performed 536 investigations and received 1,732 complaints. A total of 55 sanctions corresponding to €254,075 in fines were issued. These penalties were imposed by the DPA regarding instances of unlawful processing of personal data (Arts. 5, 6 and 9 GDPR), violations of data subject rights (Arts. 15 and 17 GDPR) and inadequate cooperation with the DPAs (Art. 31 GDPR). Two cases handled by the Austrian DPA in 2023 are worth highlighting.

In February, the Austrian DPA rejected a complaint on the grounds that it was manifestly unfounded pursuant to Art. 57(4) GDPR. Upon its investigation, the DPA uncovered that the complainant had offered to refrain from lodging a complaint with the data protection authority against a payment of €2,900. A letter from the complainant on this matter was submitted by the respondent. Against this background, the Austrian DPA concluded that no real need for legal protection can be assumed on the part of the complainant, thereby rendering the filing of the complaint as dishonest and the use of the data protection authority's activities by the complainant as an abuse of rights.

In May, a data controller located in the US, Clearview AI, was ordered by the Austrian DPA to delete the complainant's personal data and appoint a representative in the EU in accordance with Art. 27 GDPR. The data controller operates a face recognition platform that allows its customers to match photos of people with images found online. The images are gathered from websites featuring publicly accessible photos of human faces. The database at the time contained 30 billion photographs. The decision against Clearview AI was taken after the Austrian DPA established that the data controller had been processing biometric personal data contrary to Art. 5(1)(a) and (b) GDPR and without a legal basis pursuant to Art. 6(1) GDPR or Art. 9 GDPR.

3.4.2. BELGIUM

In 2023, the Belgian DPA had 85 investigation files and one specific audit regarding the Schengen Acquis. The DPA also issued 57 compliance orders and adopted 110 sanctions, including three fines corresponding to €80,000 in total. Three cases are presented in this section.

The Belgian DPA handled a case regarding the Belgian Ministry of Finance's transfer of personal banking data to the US tax authorities (IRS) in the context of the application of the "FATCA" intergovernmental agreement between Belgium and the United States. The Litigation Chamber of

the Belgian DPA concluded that the processing of personal data by the Ministry of Finance, including their transfer to the IRS, was unlawful, as it violated the principles of purpose, necessity and minimisation, as well as the rules of Chapter V of the GDPR (lack of appropriate safeguards for the transfer to the US, as set out in the FATCA agreement). In view of the unlawfulness of the processing, the Litigation Chamber mandated the cessation of processing the complainant's data. While the Brussels Court of Appeal later granted the Ministry's request for suspension of the decision, it referred the case back to the Litigation Chamber on 20 December 2023.

In another case, the Belgian DPA concluded that the collection and listing of personal data by an online platform, such as contact details and professional status, was unlawful. Indeed, the DPA considered that the condition of balancing the opposing rights and interests at stake was not met. More specifically, it ruled that the processing by the data controller did not fall within the reasonable expectations of the individuals. Lastly, the Belgian DPA concluded that the right to data erasure was not implemented in a timely manner under Art. 12(3) GDPR. The data controller was therefore issued a fine of €10,000 and was ordered to cease the unlawful processing. It should be noted that an appeal for annulment has been lodged against this decision with the Brussels Court of Appeal.

Finally, the Belgian DPA issued an administrative fine of €40,000 to a data controller for the violation of the complainant's right of access, specifically to recordings of telephonic conversations. The complainant had entered into two agreements with the data controller under which the defendant would be responsible for developing a website and corporate videos for the complainant. In connection with these agreements, telephone conversations took place regarding the functional elaboration and design of this website and videos. However, the complainant claimed that he was not aware of the recording of such conversations. The Belgian DPA ruled that the recording of the phone calls was lawful as (a) the requirements under Art. 6(1)(b) GDPR were met and (b) the complainant had been properly informed about the processing. However, the Belgian DPA concluded that the data controller infringed the complainant's right of access by omitting to provide a copy of the phone call recordings. In addition to the fine, an order to provide the recordings to the complainant was issued.

3.4.3. BULGARIA

The Bulgarian DPA, the Commission for Personal Data Protection (CPDP), dealt with 1,497 complaints and performed 890 investigations in 2023. 93 sanctions were issued, corresponding to €159,931 in fines. Complaints addressed by the DPA pertained to data breaches concerning travel arrangements, commercial payments with virtual currencies, and on-line sales, as well as the processing of personal data regarding video surveillance, political campaigns, sensitive data, telecommunications, postal services, etc. This section will cover a selection of these cases.

In 2023, the Bulgarian DPA handled a case concerning a fine issued by another Member State authority in response to traffic regulation violations by an individual with a business vehicle. At the time of the violation, the individual was on sick leave and when the fine was issued, the individual was no longer an employee of the data controller. Upon receiving the fine, the data controller's official failed to check the circumstances of the traffic violation and provided the individual's personal information to the issuing authority. The vehicle was used based on a concluded contact between the data controller and the leasing

company. On the date of the violation, the vehicle was in possession of the leasing company with which the individual had no relations. In light of this, the CPDP issued a property sanction of BGN 10,000 (approximately €5,000). The case can be found on the following link: https://cpdp.bg/userfiles/file/Bulletin/KZLD_Bulletin_2_101_March_2023.pdf - in Bulgarian - pages 50-58.

In another case, the Bulgarian DPA imposed a fine of BGN 25,000 (approximately €12,500) on a data controller for the violation of Art. 6(1) GDPR. The data controller was ordered to take the necessary technical and organisational measures to bring its processing operations in compliance with the GDPR. This decision was taken by the Bulgarian DPA in relation to a political party's submission of a list with names of supporters to participate in the Parliament elections. When submitting the list, the political party failed to implement clear procedures for verifying the personal identification data contained therein. As a result of this and considering the party's repeated violations of the same nature in the past, the Bulgarian DPA decided to issue the data controller a hefty fine (https://cpdp.bg/userfiles/file/Bulletin/KZLD_Bulletin_2_101_March_2023.pdf - in Bulgarian- pages 28-35).

3.4.4. CROATIA

In 2023, the Croatian DPA performed 447 investigations, received 279 complaints, issued 148 compliance orders, and adopted 28 sanctions corresponding to €8,266,350 in fines. These relate among others, to data breaches due to a lack of undertaking appropriate technical and organisational measures, the processing of personal data concerning CCTV, processing of sensitive data without a lawful basis, not providing transparent information to individuals about the processing of their personal data, the absence of a data processing agreement between a data controller and data processor etc.

There are three cases worth highlighting.

The Croatian DPA imposed an administrative fine of €5,470,000 (HRK 41,213,715) on a debt collection agency acting as a data controller. This penalty was imposed for breaches of Arts. 5, 6, 9, 12, 13, and 26 of the GDPR.

The Croatian DPA imposed an administrative fine of €2,265,000 on a debt collection agency as a data controller. This fine was issued in response to violations of Arts. 13, 28, and 32 of the GDPR.

The Croatian DPA issued an administrative fine of €380,000 to a trading company for organizing betting games acting as the data controller. This penalty was imposed for violations of Arts. 6, 13, 25, and 32 of the GDPR.

3.4.5. CYPRUS

In 2023, the Cyprus DPA received 437 complaints, 130 of which related to unsolicited electronic communications. The DPA performed 14 investigations and 11 of them were carried out with on-site inspections. It issued 54 Decisions, which included 8 compliance orders and 11 fines corresponding to €120,250. These fines were imposed for data breaches concerning cyberattacks, as well as for processing personal data without a valid legal basis or without appropriate technical and organizational measures in place.

The first case of interest occurred in March and concerned a personal data breach involving a ransomware cyberattack. The Cyprus DPA was notified about this incident by the Open University of Cyprus. According to the university, the personal data of students, graduates and contractors that

was stored on a file server, which included copies of identification cards and medical data, was leaked and made available on the dark web. Against this background, the DPA concluded that the data controller infringed Arts. 5(1)(f), 24 and 32 GDPR for the lack of appropriate security measures, as well as Art. 5(2) GDPR (accountability). An administrative fine of €45,000 was issued to the data controller, along with an order to appoint a security officer and inform the Cyprus DPA about the progress of the implementation of additional security measures within six months of the decision.

The second case handled by the Cyprus DPA pertained to the communication of personal data from the Ministry of Interior to the House of Representatives, following a request in the context of the parliamentary scrutiny. The Cyprus DPA issued a fine of €8,000 for the infringement of Art. 5(1)(a), (c) and (f) GDPR. The Cyprus DPA concluded that the public authorities had violated GDPR provisions by using dedicated and confidential forms to collect personal data of employees and Advisory Committee members of the T/C Properties Management Service, which were later found to have been published in a daily newspaper. These forms had been communicated by the Ministry to the requesting Parliamentary Committee in a manner that did not ensure appropriate security of the personal data.

Finally, the Cyprus DPA received 37 complaints in 2023 concerning spam SMSs and telephone calls sent by the campaign headquarters of the later-elected President of the Republic. The headquarters claimed that during the campaign thousands of citizens provided their personal data and consented to receiving informational material from the headquarters' staff. However, the Cyprus DPA uncovered that because of the volume of phone calls made and SMSs sent during the campaign, staff had mistakenly contacted individuals who had not provided their consent. The Cyprus DPA concluded that Art. 106 of Law 112(I)/2004 and Arts. 5(1)(a), (b) and 6(1)(a) GDPR were violated. A total fine of €36,000 was levied for the reported complaints. Furthermore, the Cyprus DPA issued two fines of €3,000 and €2,000 to two other persons for seven complaints linked to the same candidate.

3.4.6. CZECH REPUBLIC

In 2023, the CZ DPA performed 27 investigations, received 1,134 complaints, issued 25 compliance orders, and imposed 23 fines in the amount of CZK 3,658,000 (approximately €140,000). These related, among others, to the processing of personal data via cookies (insufficient legal ground, insufficient compliance with the information obligation), failure to notify and to communicate a data breach, processing of personal data in police databases, lack of personal data security or providing third persons with access to customer databases.

A court has already confirmed a fine of CZK 140,000 (approximately €5,700) that the Czech DPA imposed on the grounds of the Czech Republic´s specific legislation related to processing of personal data within a criminal proceeding on a publishing company. The act under consideration consisted of disclosure of information originating from interception and records of telecommunication traffic of active high-ranking politician. A strictly individualized proportionality test between the public interest to inform and the privacy protection concern proved to be a key element. The CZ DPA´s competence to conduct the proceeding is not subject to the lodging of a complaint and investigation may therefore be exercised *ex officio*.

It can be taken for granted that a publicly active high-ranking politician cannot be in any way stripped from the right to privacy, however the public interest in information necessary for the formation of political opinions among the public or for the overall assessment of the politician can prevail over the person´s interest for protection of privacy. Concurrently, special considerations shall be taken as to the rights of other individuals who are not publicly active (for example assistants or drivers) and who could be disproportionately affected by the disclosure of the interception.

The method and context of publication are also important. Information therefore cannot be presented in a coarsely insulting manner or, respectively, as an attempt to create a sensation even if it would be a verbatim transcript of communications. The fact that similar information has already been published does not pose any obstacle for a sanction proceeding.

In 2023, the CZ DPA imposed a fine, under the Law Enforcement Directive, on the Ministry of Interior of the Czech Republic in the amount of CZK 975,000 (approximately €39,800) for a large-scale processing of personal data by the Police of the Czech Republic concerning persons ordered to isolation due to the ascertained COVID-19 disease. Affected by the processing were approximately 2,000,000 individuals who were infected by the disease between 1st April 2021 and 8th March 2022.

The Police collected personal data on the individual´s health state on a large-scale and preventively without any linkage to a specific investigated case whereby it exceeded its competence vested by the national legislation for processing of personal data.

Furthermore, the Police failed, in this respect, to properly meet the information obligation towards persons whose personal data were collected and processed in relation to the ascertained COVID-19 disease. Yet another breach consisted in omitting of two steps foreseen by the law that should have to precede the start of such a vast and serious collection of personal data. The police should have had to carry out a data protection impact assessment (DPIA) in the first place. The intended manner of the large-scale gathering and processing of personal data on health should have had to be consulted beforehand with the CZ DPA. The law declares these two steps as obligatory for that kind of personal data processing, namely as a risk prevention in case of persons whose data shall be processed.

Link to annual report of CZ DPA: https://uoou.gov.cz/media-publikace/ke-stazeni/vyrocni-zpravy

3.4.7. DENMARK

In most EEA jurisdictions, DPAs have the power to issue administrative fines. In Denmark, however, this is not the case. Indeed, data protection law infringements are first looked into by the Danish DPA before being reported to the police. After the police has conducted an investigation to determine whether charges should be filed, the court then decides on any possible fines. In 2023, the Danish DPA performed 504 investigations, received 1,765 complaints, and proposed 5 sanctions of at least €2.1 million in fines. Two cases are worth highlighting in this section.

In the first case, a reprimand was issued to the Danish Agency for Digitalisation for violating the data minimisation principle laid down in Art. 5(1)(c) GDPR. The Danish DPA established that the Agency had processed the personal data of far too many Danish citizens (almost four million) when running its application containing digital replicas of citizens' driving licences. The DPA concluded that

the Agency's processing activities in connection with the operation of the app, whereby an extract of information about all holders of a valid Danish driving license in the official driving license register, which is run by the Danish Police, is stored and processed, is not in accordance with the GDPR. Consequently, the DPA prohibited the Agency to further store and otherwise process personal data from the official driving license register about citizens who had not actively signed up to use the application.

The Danish DPA opened a case against the Danish Growth Fund (DGF) on the basis of a complaint from a citizen. According to the complainant, the DGF used spy pixels in its newsletters, allowing it to collect data on the recipients' online behaviour. The DGF specifically used this method to track which articles the recipients clicked on, in order to optimize the organisation and sending of their newsletters. However, the consent of the recipients had not been obtained by the DGF for processing data through the use of spy pixels. Furthermore, the DPA established that the data controller failed to observe the obligation to provide information regarding the processing of the recipients' data. For the reasons mentioned above, the DGF was issued a reprimand.

3.4.8. ESTONIA

In total, the Estonian Data Protection Inspectorate (EDPI) received 833 complaints and 193 data breach notifications affecting over 322,229 individuals in 2023. The EDPI issued 383 compliance orders, conducted 53 own initiative inspections and adopted 12 sanctions corresponding to €213,300 in fines and penalty payments.

The EDPI issued a fine of €200,000 to the Ida-Tallinna Central Hospital for its failure to ensure the appropriate security of the health data of their patients, specifically the protection of that data against unauthorised or unlawful processing. It was established by the Estonian DPA that no internal regulation to destroy paper records of health data had been put in place by the data controller. Pursuant to the complaint, the health data of several patients was made available to all passers-by in an open container next to the hospital's main door.

In 2023, the Estonian DPA also dealt with a case concerning the processing of data of childless women by the Pere Sihtkapital Foundation. It was revealed that the foundation had requested the Population Register for the contacts of childless women and then proceeded to inquire them about sensitive matters, such as their political party affiliation. The data collection on women was conducted by an employee of the University of Tartu, however it was established that the employee in question had exceeded its competence when concluding the cooperation agreement. The Estonian DPA concluded that the Pere Sihtkapital Foundation failed to inform the data subjects in a timely manner and to fulfil the obligation to provide information regarding its processing activities. The data controller was consequently instructed by the EDPI to delete the processed data. Misdemeanour proceedings against the foundation are underway.

Lastly, the EDPI is presently in the midst of misdemeanour proceedings against the Viljandi Hospital. According to the case facts, hospital employees were asked to provide a urine sample in order to reveal the individual responsible for the theft of medicine from the hospital's medicine cabinet. However, several employees expressed that they had not given their concrete consent to provide the urine sample.

3.4.9. FINLAND

In 2023, the Finnish DPA performed 11 inspections, received 1,763 complaints, issued 20 compliance

orders and adopted three sanctions corresponding to €464,600 in fines. These relate, among others, to the right of access regarding phone calls or patient records as well as failing to comply with the DPA's order. In this section, three cases from the Finnish DPA's work related to data protection violations are presented.

On the basis of non-compliance with an order issued by the Finnish DPA, a credit information company, Suomen Asiakastieto Oy (data controller), was awarded a fine of €440,000. The Finnish DPA had ordered the data controller to rectify its practices in registering payment default entries and to erase all inaccurate entries saved into the credit information register due to inadequate practices. The Finish DPA established that information based on decisions issued in civil cases should not have been registered as payment default entries.

The Finnish DPA issued an administrative fine of €23,000 on a business directory operator, Suomen Yritysrekisteri (data controller), for infringements of the right to access regarding sales call recordings. The company had delivered a written summary of the call in some of the cases, but the summaries did not correspond to the contents of the call. The fine was also grounded in the fact that the data controller had neglected to comply with the DPA's prior order to rectify its practices.

The accommodation provider Forenom (data controller) was issued a reprimand for the lack of sufficient safeguards and an order to shorten its data retention period. The data controller was subject to a data breach that affected the personal data of tens of thousands of customers in several EU countries. The protection measures of the data controller were inadequate, and the data controller had not complied with the principles of data minimisation and storage limitation. The matter was processed in cross-border cooperation with 17 Concerned Supervisory Authorities (CSAs).

3.4.10. FRANCE

In 2023, the French DPA, the National Commission on Informatics and Liberty (CNIL), handled several cases where it issued a total of 37 sanctions corresponding to €79,164,500 in fines relating to, among others, information given to individuals, consent of individuals, security of personal data and lack of cooperation with CNIL. It was established that the CNIL performed 157 on-site inspections and 183 other investigations, received 16,431 complaints and issued 55 compliance orders in 2023.

On 13 April, the CNIL dealt with a national case where it imposed an overdue penalty payment on Clearview AI. The company was ordered to pay €5,200,000 for having failed to comply with the order issued as part of the DPA's sanction decision of October 2022.

On 15 June, the CNIL sanctioned CRITEO, which specialises in online advertising, with a fine of €40 million for failing to verify that the persons from whom it processed data had given their consent. This case was dealt with through the OSS mechanism with CNIL as Lead Supervisory Authority (LSA) and all other DPAs as CSAs.

3.4.11. GERMANY

There are both national (federal) and regional DPAs in Germany. Three cases are highlighted in this section. A case was addressed by the Saxon Data Protection and Transparency Commissioner (Saxon DPA) concerning the permanent monitoring of children's communications by a company offering internet services. The Saxon DPA uncovered that the data controller was providing its internet services without age verification measures to children between the ages of 12 and 18. Moreover, upon the individual's

entry on the internet platform, several external services by third parties were initiated without the user's consent. The data controller had later introduced an age verification by self-declaration, but the Saxon DPA ruled it to be ineffective. In the end, the Saxon DPA deemed the consent of the children invalid and issued a reprimand to the controller.

In another case, the Lower Saxony DPA carried out investigations, including on-site inspections, regarding so called "smart data analytics" by several banks. Such analytics are utilised to filter out specific individuals from the customer base for certain advertising measures. The scores generated were particularly based on payment transaction data, as well as a wide range of other personal data, such as the customer's age, personal status, and the duration of the customer relationship. In most cases, the banks based the processing on "legitimate interests" under Art. 6(1)(f) GDPR. However, the Lower Saxony DPA conducted a balancing of interests and concluded that the fundamental rights of the customers prevailed. The Lower Saxony DPA exercised its corrective powers.

"Banks hold sensitive customer data and therefore have a high level of responsibility. We will continue to monitor this area closely."

Denis Lehmkemper, the State Commissioner for Data Protection of Lower Saxony.

In February 2023, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) issued a decision to the Federal Press Office (BPA) which prohibits the BPA to further operate the Facebook page of the German Federal government.

Upon receipt of the decision, BPA had four weeks to deactivate its Page or to bring an action against the decision before the administrative court. The BPA decided on the latter option. The Court is currently deciding the case. Since 2019, BfDI has often pointed out that it is not possible to operate a page in compliance with data protection regulations. A short report by the German Data Protection Conference underlines this assessment.

3.4.12. GREECE

The Greek DPA received over 1,328 complaints in 2023 and performed 12 on-site inspections pertaining to, among others, the following issues: a) lack of cooperation with the DPA, b) unauthorised and unlawful processing, c) non-fulfilment of data subjects' rights, d) lack of notification of a personal data breach, and e) lack of appropriate technical and organisational measures and necessary safeguards during processing. In 12 cases, the Greek DPA adopted sanctions corresponding to €636,000 in fines. Furthermore, it issued a total of 11 compliance orders.

In 2023, the Greek DPA imposed a fine on a computer systems design and related services company, Intellexa S.A., for failing to cooperate with its requests for information, after the Greek DPA had carried out an administrative inspection at the company's premises. The inspection was conducted with the intention of investigating instances of installation of spyware on mobile terminal equipment. It was determined that the company was using the spyware to monitor their users, without their knowledge, and subsequently collecting and processing their personal data. As the

company was excessively late in answering the Greek DPA's questions and did not provide any of the specific information requested, the Greek DPA imposed a fine of €50,000. Furthermore, it ordered the company to deliver the specific information immediately.

In another national case, the Greek DPA issued a €210,000 fine to the leading bank in Greece, Piraeus Bank. The bank received the fine for processing the personal data of its customers in breach of the principle of lawfulness and for failing to integrate appropriate technical and organisational measures to process only necessary data for specific purposes. Additionally, the bank infringed the complainant's right to be informed and right of access in relation to the transfer of their personal data to the Company for the Management of Claims from Loans and Credits, given that there was no longer any claim against them. The investigation is currently still in progress.

Lastly, the Greek DPA dealt with a case relating to the protection of personal data processed in the framework of the Automatic Fee Collection System, also referred to as "electronic ticket". According to the DPA's inspection, the Athens Urban Transport Organisation's data processing activities violated Art. 5(1)(e) GDPR. As a result, the data controller was fined €50,000 and received a reprimand for the breaches of Arts. 25(1) and 35(1) GDPR. Furthermore, the Greek DPA issued a compliance order for the determination of data retention periods for the various purposes of processing, as well as for a revision of the impact assessment on personal data.

3.4.13. HUNGARY

In 2023, the Hungarian DPA performed 1,404 inquiries and 404 authority procedures for data protection, received 1330 complaints, issued eight compliance orders and adopted 95 sanctions corresponding to €1,380,334 in fines. Two noteworthy cases are presented in this section.

In a case related to the use of 32 cameras in rooms where facial and body treatments as well as medical aesthetic procedures were carried out, a beauty parlour was fined HUF 30 million (approximately €78,547) by the Hungarian DPA. It was uncovered that the cameras placed in the treatment rooms were oriented towards the cosmetic beds where customers would receive treatments and that sound recording was enabled. Although the company informed individuals about the video recording, they failed to provide any information on the sound recording and the genuine purpose of the surveillance. Considering the aforementioned discoveries, the DPA concluded that the data controller had violated several GDPR provisions, notably Arts. 5(1)(a) and (b) and 6(1) GDPR by continuously recording work and monitoring guests, Art. 13(1) and (2) GDPR by incorrectly and misleadingly informing the data subjects about the handling of their personal data, as well as Arts. 5(1), 24 and 25 GDPR by failing to provide the default settings for the operation of the camera system that minimise data processing. Lastly, the Hungarian DPA established that the data controller violated Art. 32(1)(b) and (2) GDPR for the lack of system security measures and Arts. 6 and 9(2) GDPR by recording the health data of the guests. In addition to the fine issued, the DPA prohibited video surveillance in all rooms and ordered the erasure of video recordings, customer health-related data and any data generated from the recordings.

The Hungarian DPA received several complaints concerning the processing practice of a retail chain in relation to the purchase of alcoholic drinks. When purchasing alcoholic drinks in the shop of the chain, buyers regardless of being of legal age to purchase alcohol were mandated to provide an ID card with a photograph. The complainants argued that privacy statements were not provided to them upon their request and hence the legal

basis of processing and its duration was unknown to the customers in relation to the recording of birth dates. In its decision, the DPA held that the data controller infringed the principles of transparency and data minimisation under Art. 5(1)(a) and (c) GDPR, as well as violated Arts. 12 and 13 GDPR in the context of informing the data subjects. Finally, the data controller did not have a legal basis for processing under Art. 6 GDPR and failed to apply data security measures pursuant to Art. 32(1) and (4) GDPR. As a result, the data controller was issued a fine of HUF 95 million (approximately €248,732) and was ordered to review its age verification practice and display a privacy notice at its premises.

3.4.14. ICELAND

In 2023, the Icelandic DPA carried out 127 investigations, received 105 complaints, and imposed 12 sanctions, corresponding to €537,000 in fines.

In October 2021, the EDPB selected the use of cloud services in the public sector for its 2022 Coordinated Enforcement Action. The Icelandic DPA decided to investigate the use of cloud services in elementary schools within the five largest municipalities in the country as part of this coordinated action. The municipality of Kópavogur was issued a fine of €26,675 for the processing of personal data within the Seesaw educational system for multiple violations against GDPR provisions, notably failure to demonstrate a legal basis for all processing operations (Art. 6 GDPR), failure to comply with the principles relating to processing of personal data (Art. 5 (a), (b), and (c)) and data transfers to the United States without appropriate safeguards (Arts. 44 and 46 GDPR), among other breaches.

The Icelandic DPA imposed its most significant fine to date, corresponding to €244,933, to Creditinfo, a service provider for credit information and risk management solutions. The company failed to comply with the obligation to process personal data lawfully, fairly, and in a transparent manner by recording defaults deriving from short-term loan providers without the necessary loan terms being presented (Arts. 5(1)(a) and 5(2) GDPR). The company also failed to demonstrate a legal basis for their processing operations by registering claims in their default registry that were below the required minimum amount (Art. 6(1) GDPR).

The Icelandic DPA considered the following aggravating factors in the case: (1) the number of registered data subjects; (2) the fact that the data processing was related to the firm's core business; (3) the fact that the data processing was intended to generate profit; (4) the delay in deleting registrations after the unlawful processing was revealed; and (5) the severe nature and consequences of the processing for the data subjects.

3.4.15. IRELAND

In 2023, the Irish DPA (Data Protection Commission, or 'DPC') handled 2,600 complaints, issued 19 compliance orders and adopted six national fines corresponding to €1,282,500 of fines in total, in addition to over €1.5 billion in cross-border fines issued by the DPC in 2023.

In February, an inquiry was commenced by the Irish DPA after being notified by the Bank of Ireland 365 (BOI) of a series of 10 data breaches relating to its banking app BOI365. The data breach notifications concerned individuals gaining unauthorised access to other people's accounts via the app. The Irish DPA, after conducting its investigation, found that BOI had infringed its obligations under Arts. 5(1)(f) and 32(1) GDPR as the technical and organisation measures in place at the time were not sufficient to ensure the security of the personal data processed on the BOI365 app. As a result, BOI was imposed a fine of €750,000.

In June, the Irish DPA conducted an inquiry following public allegations in 2021 that the Department of Health had unlawfully collected and processed personal data about plaintiffs and their families in special educational needs litigation. The Department told the Irish DPA that they processed this personal data for the purposes of determining whether an approach should be made to the plaintiff to seek to settle the case. However, on the files examined the Irish DPA found evidence that the Department had infringed data protection law by asking broad questions that resulted in the provision of sensitive information about the private lives of plaintiffs and their families. Furthermore, the Irish DPA determined that the processing of information obtained in response to broad scoping questions sent to the Health Service Executive for the purposes of seeking to settle a case was excessive and disproportionate to the aims pursued. Additionally, the processing for this reason was not necessary for the purposes of litigation. Therefore, the Irish DPA found that there was no lawful basis for this processing in the files examined, and that the Department had infringed the principle of data minimisation by processing the personal data. As a result, the Department was imposed a fine of €22,500 and a ban on further processing. During the inquiry itself, the Irish DPA found infringements of transparency obligations under the GDPR and of the requirements to process personal data securely. In addition to the fine and ban on processing outlined above, a reprimand was imposed for all the infringements.

Two months later, the Irish DPA instituted temporary bans on the Galway County Council, prohibiting the processing of personal data through CCTV cameras, ANPR cameras as well as through body-worn cameras. The Council was also issued a reprimand in respect of the Council's violation of Art. 24 GDPR and an order to bring its processing into compliance with the GDPR. The Irish DPA came to this decision after examining a number of the Council's processing operations including its use of CCTV cameras in public places for inter alia the purposes of prosecuting crime. The Irish DPA found that the Council lacked a valid legal basis for processing personal data from the cameras and failed to erect appropriately worded signage in respect of the processing of personal data via the CCTV cameras for purposes related to law enforcement.

3.4.16. ITALY

The Italian DPA, Garante per la protezione dei dati personali, performed investigations into several thousands of cases in 2023. It also received over 10,000 complaints, issued 221 compliance orders and adopted 146 sanctions corresponding to €25.2 million in fines. These relate, among others, to infringements of data subject rights, unlawful telemarketing, and data breaches affecting public and private bodies. Two especially noteworthy cases are presented in this section.

The Italian DPA took action against OpenAI, the US-based company behind ChatGPT. The Italian DPA temporarily limited the processing of data belonging to Italian users, following a reported data breach involving ChatGPT. It also initiated an inquiry into several points of concern: the lack of information to users; the unclear legal basis for the extensive collection and processing of personal data used to train the platform's algorithms; the risks arising from the processing of inaccurate personal data; and the absence of an effective age verification mechanism. OpenAI took several steps in response to the Italian DPA's concerns, such as updating the privacy policy and providing opt-out options for users; however, additional efforts were found to be necessary regarding age verification. This led, among other things, to the setting up of an ad-hoc task force by the EDPB to address such issues in a coordinated manner at the EEA level.

In another case, several measures against aggressive telemarketing practices were taken by the Italian DPA. The measures encompassed three significant interventions that resulted from distinct investigations. In the telecommunications sector, a TELCO operator was fined over €7 million. Similarly, in the energy sector, two companies received fines of almost €250,000 and €700,000, respectively. In the case of TELCO, lack of oversight on unauthorised call centres not affiliated with their official network was a key concern. Additionally, issues related to the exercise of data subjects' rights and the unauthorised publication of personal data in public telephone directories were raised. A national Code of Conduct was also adopted to regulate telemarketing and teleselling activities. The Code envisages specific commitments such as obtaining explicit consent for each purpose of data processing, providing clear and precise information to individuals regarding the intended use of their data, and guaranteeing the exercise of privacy rights (right to object, right to rectification). Furthermore, the Code requires that contracts between operators and service providers should include penalties for any service sales that are conducted without obtaining proper consent from customers.

3.4.17. LATVIA

In 2023, the Latvian DPA, the Data State Inspectorate of Latvia, performed over 850 investigations. It also received 733 complaints, issued 195 compliance orders and adopted three sanctions corresponding to €22,900 in fines. The cases presented in this section focus mainly on the unlawful processing of personal data and the use of cookies.

The Latvian DPA identified non-compliance with GDPR requirements in a case related to the use of cookies on a website. After repeated inspections by the DPA, it was concluded that the data controller did not provide clear, user-understandable, and comprehensive information about the types of cookies used and their purposes on its website. Indeed, users were unable to source this information from the informational warning banner, the pop-up window, as well as the Cookie Policy. As a result of these significant deficiencies, the controller was imposed an administrative fine of €20,000.

In another case, the Latvian DPA issued a reprimand to a general practitioner for the unlawful processing of personal health data. The DPA received a complaint from an individual who discovered that their personal data had been accessed over 30 times by a staff member of a general practitioner's practice in the unified health information system. The unauthorised access involved obtaining information about the individual's medical history, prescribed medications, and more. Following Art. 18 of the Law on General Practitioners, the Latvian DPA held the general practitioner responsible for the activities of its personnel.

3.4.18. LIECHTENSTEIN

A total of 23 investigations were performed by the Liechtenstein DPA in 2023. It received 43 complaints, issued 22 compliance orders and adopted one sanction corresponding to €500 in fines relating to the controller's refusal to cooperate with the authority. Two cases are presented in this section.

In 2023, the Liechtenstein DPA received a complaint regarding the Electronic Health Records, in particular its legal basis (opt-in versus opt-out) for processing personal data, the right to information under Art. 13 GDPR as well as security safeguards. In this case, the DPA concluded that the national Law on Electronic Health Records which stipulates an automatic establishment of electronic health records with the option for every data subject to opt-out,

is legitimate and constitutes a valid legal basis for the data processing under Art. 6(1)(e) GDPR. However, the national law further provided for the processing of health data for scientific research. The Liechtenstein DPA concluded that for such processing the latter did not constitute a legitimate legal basis as in this specific case only consent could be considered legitimate. Accordingly, the Liechtenstein DPA banned the processing for such purposes and ordered the competent Ministry to amend the law in this regard. Regarding the right to information laid down in Art. 13 GDPR, weaknesses were established, however these were remediated during the proceedings. Finally, the Liechtenstein DPA decided that the safeguards put in place corresponded to the state of the art.

The Liechtenstein DPA also received a complaint regarding online job interviews. The complainant argued that there was no legal basis as they did not have a real choice between an online interview and an interview on the premises. The Liechtenstein DPA concluded that for such processing the data subject needs to freely give their consent under Art. 6(1)(a) and Art. 7 GDPR, and the data controller needs to prove that this consent was indeed provided. However, in this case, the supposed consent was only given orally, and the data controller could not prove it. Thereby, the Liechtenstein DPA concluded a violation of Art. 6(1)(a) GDPR.

3.4.19. LITHUANIA

In 2023, the Lithuanian DPA handled 1,221 complaints of individuals, 47 of them were resolved by an amicable settlement, performed 46 investigations, finished 95 monitoring procedures, received and investigated 254 notifications of personal data breaches. Lithuanian DPA imposed 13 fines, the total amount of which is € 64,060. Three noteworthy cases are presented further.

On 20 April, the Lithuanian DPA investigated a personal data breach in the information system of a private company providing cleanliness services. The company was fined €20,000 for failing to comply with the data storage time limitation and confidentiality principles laid down in Art. 5(1)(e) and (f), Art. 31(1)(b) and (d) GDPR.

On 11 September, the Lithuanian DPA issued administrative fines to a private healthcare company and a doctor working there for publishing a patient's photographs on a social network, thereby violating Art. 5(a) and (f), Art. 6(1) and Art. 9(2) GDPR. The doctor was fined €840, while the private health care company received a fine of €6,000.

On 6 December, the Lithuanian DPA investigated a complaint concerning the non-implementation of the right to erasure and the unlawful processing of the complainant's personal data (videos) on an Instagram account managed by a private company. The data controller affirmed that the complainant's data would be erased only if compensation was provided to the company for financial losses related to the removal of the records. However, the Lithuanian DPA argued that compensation for damages suffered by the data controller does not constitute a valid condition for withdrawal of consent. The Lithuanian DPA concluded that the data controller violated Art. 5(1)(a), Art. 12 and Art. 17(1) GDPR and ordered the company to delete the videos of the applicant from the company's Instagram account.

3.4.20. LUXEMBOURG

The Luxembourgish DPA received 552 complaints in 2023, and as a result thereof performed a total of 21 investigations. It issued three compliance orders and seven reprimands, along with three sanctions totalling €6,500. Two national cases handled by the Luxembourgish DPA in 2023 are presented in this section.

A data controller offering electronic communication services was issued an administrative fine of €1,500 for violating Art. 13(1)(e) and Art. 24(1) GDPR. The Luxembourgish DPA concluded that the controller had failed to provide information about the recipients of the personal data. In its decision, the Luxembourgish DPA ordered the controller to bring its processing operations into compliance with Art. 24(1) GDPR, notably by putting in place appropriate technical and organizational measures to guarantee that the data processor ceases the transfer of the complainant's data to a third party.

In another national case, the Luxembourgish DPA concluded that the geo-tracking system put in place by a data controller violated Art. 5(1)(b) and Art. 13 GDPR. Ultimately, the data controller was issued an administrative fine amounting to €2,500 and was ordered to bring its processing operations into compliance with Art. 13 GDPR. The DPA particularly required that the data controller individually informs the employees in a clear and precise manner about the geo-tracking system.

3.4.21. MALTA

In 2023, the Maltese DPA performed 67 investigations, received 1,025 complaints and adopted three sanctions corresponding to €32,500 in fines relating to the infringement of data protection rights.

Three cases are presented in this section.

In 2023, the Maltese DPA saw an exponential rise in the number of data protection complaints, with an increase of 400 complaints over the previous year. Most of these complaints pertained to alleged infringements of data protection rights, in particular, the right of access laid down in Art. 15 GDPR. The majority of these complaints were lodged against companies operating in the online gaming industry. This increase was also reflected in the number of complaints received pursuant to Art. 60 GDPR, with an increase of Art. 63 GDPR complaints over the previous year. However, the number of personal data breaches notified in accordance with Art. 33(1) GDPR remained consistent with the previous year. The breaches which were most notified related to the unauthorised access to, or disclosure of personal data as a result of cyber-attacks suffered by controllers.

In March 2023, the Maltese DPA imposed an administrative fine of €20,000 on the public authority responsible for transport in Malta. The data controller notified the Maltese DPA of a personal data breach following a hacking attack, which affected all of its IT systems and resulted in 299,321 compromised records. The Maltese DPA found that the controller infringed Art. 32(1) and (2) GDPR for failing to implement appropriate security measures and to consider the risks presented by the processing.

Two months later, the Maltese DPA imposed another fine of €5,000 on a public authority which unlawfully recorded the private conversations of its employees by means of a CCTV camera installed at the workplace. The Maltese DPA found that the data controller processed the audio recordings without a valid lawful basis and ordered the data controller to stop the processing operation without undue delay. These two fines were imposed in line with national legislation which was introduced to implement the provisions of the Regulation, more specifically, pursuant to Art. 21 of the Data Protection Act (Cap. 586 of the Laws of Malta).

In August 2023, the Maltese DPA ordered an insurance company to revise its policy's terms and conditions together with the claim form, after it uncovered that the data controller was requesting the data subjects to submit a copy of test results for the purpose of processing a refund for a health claim. The Maltese DPA concluded that the data controller infringed the principle of data minimisation when

it requested individuals to submit a copy of the test results in a general and indiscriminate manner.

3.4.22. NETHERLANDS

The Dutch DPA finalised 16 investigations in 2023 and recorded a total of 12,342 complaints. Furthermore, three decisions imposing compliance orders were issued by the DPA along with eight decisions imposing financial sanctions corresponding to €243,160,000 in fines. These relate, amongst others, to the legal basis for the processing of personal data, insufficient transparency about data processing, security of data processing, processing of personal data by governmental institutions, and data protection impact assessments.

In 2023, the Dutch DPA was designated by a parliamentary mandate as the coordinating authority regarding algorithm supervision in the Netherlands. This task was allocated to the Dutch DPA with a view to better protect public values and fundamental rights when developing and using algorithms in general, including the use of AI. The focus is to prevent discrimination, arbitrariness and promote transparency, as well as examine the fairness of algorithms and avert the spread of deceptive or misleading information.

In July 2023, the Netherlands Employees Insurance Agency (UWV) which handles unemployment benefits, informed the Dutch DPA that it had illegally collected data from benefit recipients. The usage behaviour of these recipients on the UWV's website was continuously monitored by the agency, with the underlying goal of investigating whether they were illegally staying abroad while receiving benefits. UWV recognised its violation of the GDPR and indicated that it stopped the data processing after legal consultation. The Dutch DPA ordered the UWV to take the necessary steps to inform those involved that their data was wrongfully used. Additionally, UWV agreed on the instigation of the Dutch DPA that all past and ongoing benefits fraud investigations (703 cases in total) that were linked to this breach would be reviewed. In this regard, it was established that several individuals had indeed sustained damage and consequently the UWV was ordered to compensate them.

The Dutch DPA's recent audits and inspections of the SIS and VIS revealed shortcomings in the legitimacy of processing personal data in the N-SIS and national case management systems that are connected to the VIS. As a follow-up, enhancement programs were agreed with the relevant data controllers and processors, the implementation of which was closely monitored by the Dutch DPA. The identified shortcomings were sufficiently addressed, and the programs were completed with satisfactory results in 2023.

3.4.23. NORWAY

In 2023, the Norwegian DPA carried out 119 investigations on matters related to: a) individual's right to information, access and erasure in relation to a business' processing of customer data, b) unlawful access of email-accounts and c) security of personal data processing. It received 591 complaints, issued 23 compliance orders and adopted seven sanctions corresponding to approximately €8.5 million in fines. In one case, a coercive fine of €7.1 million was imposed on a company, in line with the Norwegian Personal Data Act.

In cooperation with the Swedish, Danish and Finnish DPAs, through the OSS mechanism, the Norwegian DPA serving as LSA imposed a hefty fine on the Nordic fitness chain SATS. The chain was issued a fine of €850,000 for having violated multiple GDPR provisions, notably the individuals' right to information, access and erasure and failing to identify a legal basis for processing certain personal data.

In July, the Norwegian DPA urgently imposed a temporary ban on Meta IE. The ban was related to the company's practice on behavioural marketing on Facebook and Instagram, which the Norwegian DPA considered to be illegal. The Norwegian DPA issued Meta IE a coercive fine of €7.1 million for failing to comply with the ban, pursuant to the Norwegian Personal Data Act. Additionally, the Norwegian DPA opted to elevate the case to the European level and requested an urgent binding decision from the EDPB. In November, the EDPB decided that the Norwegian ban on behavioural marketing on Facebook and Instagram should become permanent and extend to the entire EU/EEA.

3.4.24. POLAND

In 2023, the Polish DPA actively performed 46 investigations which resulted in the issuance of 31 compliance orders and the adoption of 24 sanctions corresponding to €213,820 in fines. It received a total of 5,288 complaints. This section takes a closer look at two relevant cases from 2023.

In the case involving a failure to notify a personal data breach affecting the rights and freedoms of natural persons, the Polish DPA issued a fine of €22,000. The Polish DPA was informed that an unauthorised recipient had received a document in an email attachment from an insurance company, Link4 Towarzystwo Ubezpieczeń S.A., containing personal data such as first name, last name, mailing address, registration number of the car and value or amount of the claim awarded. The insurer had made a risk analysis based on ENISA's recommended methodology and the analysis showed low risk to the rights of individuals, thereby it resigned from notifying the breach to the Polish DPA. The Polish DPA stated, however, that in the case there was an obligation of such a notification and therefore there was a violation of the GDPR provisions.

Link: https://www.uodo.gov.pl/en/553/1581

The Polish DPA imposed another significant fine in 2023 for the failure to notify a personal data breach to the supervisory authority. This case concerns an incident where a local journalist who after receiving non-anonymised documentation from the District Public Prosecutor's Office, proceeded to publish the documents on a local website. This resulted in a breach of the confidentiality of individuals' data as the documents had been improperly anonymised. Taking into account the wide range of data disclosed, the Polish DPA imposed an administrative fine of €4,500 on the District Prosecutor's Office for failing to notify the personal data breach to the Polish DPA and the concerned individuals. The data controller was ordered to rectify this by promptly communicating the breach to the individuals affected.

Link: https://www.uodo.gov.pl/en/553/1501

3.4.25. PORTUGAL

In 2023, the Portuguese DPA initiated 1,818 investigation procedures, performed 45 inspection actions, received 1,188 complaints, issued three compliance orders and adopted 52 sanctions, which includes four reprimands and 48 fines, in the total amount of €367,450. These relate mostly to the non-compliance of data protection principles, particularly the lawfulness of data processing, violations of data subjects' rights requests, undue disclosure of personal data on the Internet, including sensitive data, and non-compliance with GDPR provisions related to data protection officer (DPO). Two kinds of cases are presented in this section.

During the COVID-19 pandemic, some municipalities disclosed information on the Internet related to people diseased and/or recovered, which were allegedly anonymised. However, the individuals were identifiable, which meant that sensitive personal data was made publicly available. Such data processing had no legal ground, and considering all the

circumstances of the case, the Portuguese DPA issued reprimands to sanction this infringement.

In other cases, the Portuguese DPA issued a significant number of fines for the failure to appoint a DPO, the lack of notification of the DPO's identification and contacts to the supervisory authority, and the organisation's neglect to publish the DPO's contact details.

3.4.26. ROMANIA

The Romanian DPA received 4,092 complaints in 2023 concerning infringements of several GDPR provisions such as lack of legal basis and violations of principles for the processing of personal data, such as confidentiality and security rules. As a result of the latter, the Romanian DPA performed 424 investigations, applied 22 reprimands, and issued 68 fines corresponding to a total amount of €444,622.

In 2023, the Romanian DPA was contacted by the Hungarian DPA through the OSS mechanism to act as LSA in a case against the controller, Dante International SA, given that the company's headquarters were in Romania. After investigating complaints submitted by three natural persons, the Romanian DPA concluded that the data controller had breached Art. 12(2) and Art. 17(1) GDPR by failing to facilitate the exercise of individuals' rights and to delete personal data without undue delay. Furthermore, since the company's website did not contain sufficient information regarding data transfers to third countries, the controller was deemed to have infringed Art. 13(1)(c), (e) and (f), as well as Art. 14 (1)(c), (e) and (f) GDPR. Lastly, the data controller breached Art. 6 (1)(a) GDPR given that it continued to process the email address of an individual subsequent to the request for its rectification and without their consent. The company was issued a global fine of €40,000 for its violations and received a reprimand. The Romanian DPA also imposed several corrective measures.

In another case, a company named Uipath SRL, notified the Romanian DPA of a significant breach of confidentiality of personal data. The Romanian DPA established that the data of over 600,000 users from 258 States (out of which 76,095 data subjects were from EU Member States) had been published on a website. The occurrence of this incident was facilitated by the data controller's failure to implement adequate security measures for its data storing spaces, thereby allowing unauthorised access to the personal data of its users. As a result, the data controller was issued a fine of €70,000.

In October 2023, the data controller Rompetrol Downstream SRL was imposed a fine of €110,000 for the breach of Art. 32(4) in conjunction with Art. 32(1)(b) and (2) GDPR, as well as Art. 58(2)(i) and Art. 83(4)(a) GDPR. According to the case facts, the company failed to take measures to ensure that any natural person acting under the authority of the data controller and that had access to personal data processed it solely at its request. Additionally, the data controller did not implement adequate technical and organisational measures to ensure a level of security corresponding to the risk of the processing, including the ability to guarantee the confidentiality, integrity, availability and continuous resistance of the processing systems and services. These shortcomings led to the unauthorised access of the personal data of 12 data subjects.

3.4.27. SLOVENIA

The Slovenian DPA handled several cases in 2023 related to the unlawful disclosure of personal data to unauthorised users, unlawful publication, and collection of personal data as well as illegal video surveillance and unlawful processing in direct marketing. In total the DPA performed 702 investigations, received 260 complaints, received 183 data breach notifications, issued

74 compliance orders and adopted 77 sanctions corresponding to €56,910 in fines. The issued fines in 2023 relate to breaches of both the national data protection act and the GDPR. Additionally, the Slovenian DPA issued 60 warnings, which are not considered as a sanction under Slovenian law.

The Slovenian DPA issued a prohibition to process personal data to delivery companies for failing to demonstrate why their processing activities were necessary to comply with road traffic rules. According to the Slovenian DPA, the companies marked the bags of deliverers with identification numbers, visible to the public. The purpose of this measure, according to the data controllers was to ensure compliance with road traffic rules, notably facilitating controls by traffic wardens and the police in the event of infringements. However, the data controllers did not provide a legal basis for this purpose.

In a second case, the Slovenian DPA assessed the lawfulness of video surveillance in a restaurant. The data controller was inter alia recording food preparation and guest tables and subsequently transmitting the live image via their website. The Slovenian DPA established that the data controller had not demonstrated the lawfulness of video surveillance in the working premises, as the recording was not strictly necessary for the security of persons and property, and the purpose of protection was already achieved by other means. Furthermore, no legitimate interest had been demonstrated. In light of this, the Slovenian DPA prohibited the transmission of the live image as well as the video surveillance of the area where food is prepared and where guests are served.

Finally, the Slovenian DPA received a complaint from an individual concerning a public authority's refusal to fulfil the persons' request for the deletion of personal data from an online registry. The registry included information about the complainant's permanent and temporary residence country. The DPA concluded that no legal basis for the publication of this data existed, and consequently held the public authority responsible for the violation of Art. 6 and Art. 17 GDPR. The data controller was ordered to make the applicant's permanent and temporary residence address inaccessible to the public on its website.

3.4.28. SPAIN

In 2023, the Spanish DPA performed 291 investigations, received 18,879 complaints, issued 266 compliance orders and adopted 367 sanctions corresponding to €29,817,410 of fines relating. These relate among other, to personal data breaches concerning large companies such as Telcos and financial institutions, infringements related to data subject rights, fraud in service contracts, debt management, etc.

In 2023, the Spanish DPA handled several cases. A few cases of particular importance are presented in this section.

The Spanish DPA dealt with a case involving the theft of an individual's purse, including their mobile phone, ID card and other documents containing their personal data. The Spanish DPA established that upon communicating this theft to the bank, the bank failed to prevent the impersonation of the person's identity and the contracting of various financial products, as well as the inclusion of the claimant in a file of defaulters. As a result, the bank was issued a total fine of €1.64 million for the infringements of Arts. 6(1), 32 and 25 GDPR. The fine was later reduced to €1,184,000.

A company named OPENBANK was issued a fine of €2,500,000 for its failure to enable secure means of

communication to provide documentation with personal data of financial nature. According to the case facts, the documentation at stake contained financial data related to the economic situation of the company's clients. The infringements identified in this case by the data controller pertained to Art. 25 and Art. 32 GDPR.

Lastly, the Spanish DPA imposed a fine of €50,000 on a data controller for its non-compliance with an access request to the records and logs generated by an alarm device installed by the company in a customer's home. The claimant who suffered a theft had requested the data controller SECURITAS DIRECT ESPAÑA S.A. to provide all logs. Nevertheless, the data controller only provided those that it considered to be personal data and claimed "trade secret" as a justification. However, in addition to the fine, the Spanish DPA ordered the data controller to respond to individual's right of access.

3.4.29. SWEDEN

In 2023, the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten, 'IMY') received a total of 3,553 complaints and launched 210 investigations. During 2023 the Swedish DPA have issued 11 administrative fines. The total amount of these fines is approximately €10,780,000.

A fine of approximately €5 million was imposed by the Swedish DPA on the digital music service Spotify for violating their customers' right to access personal data under Art. 15 GDPR. While the Swedish DPA's audit revealed that Spotify had released the processed personal data upon the request of its customers, it nevertheless neglected to provide clear information about how the data was used. This case was dealt with through the OSS mechanism with the Swedish DPA as LSA and all other DPAs as CSAs.

In another case, an insurance company Moderna Försäkringar was held responsible for failing to take appropriate technical measures to ensure a level of security commensurate with the perceived risk. IMY found that on the company's web page with price quotes, there were clickable links with URLs that led to documents with insurance information and that it was possible to access other policyholders' documents, without any kind of login, by simply replacing a few numbers in the web link. IMY could conclude that it was possible to access data of 650,000 customers. Among this data, there were health data and other data such as financial information, contact details, social security numbers and insurance holdings. The data controller was issued an administrative fine of approximately €3 million.

Finally, the Swedish DPA imposed a fine of €70,000 on a municipal school in Stockholm for the infringement of Arts. 5 and 6 GDPR. According to the Swedish DPA's investigation of camera surveillance in schools since the implementation of the GDPR, the use of cameras by the municipal school during working hours was justified in certain places to address current problems with arson. However, it ordered the school to stop recording in other areas during the daytime as it violated GDPR principles.

4. ANNEXES

4.1. DPA BUDGET AND STAFF

Each year, the EDPB gathers statistics on resources made available by Member States to the DPAs from the EEA. On 15 December 2023, at its last plenary for the year, the EDPB adopted its Contribution to the European Commission's report on the application of the GDPR under Art. 97, in which these statistics are detailed.

The EDPB called on Member States to make sure that all DPAs have the necessary resources to carry out their tasks effectively, as there are considerable challenges ahead. First and foremost, the continuously evolving technological landscape presents new data protection challenges. New legislation is also considered or has been introduced, providing additional rules to create a safer digital space and to establish a level playing field for businesses in the digital economy, such as the Digital Markets Act (DMA), the Digital Services Act, the Data Governance Act or the proposal for an AI Act. These new legislations may place additional responsibilities on DPAs or the EDPB with regard to enforcement and supervision. In addition, both the EDPB's and DPAs' tasks under the GDPR continue at an increased intensity. Moreover, increased enforcement cooperation among DPAs, which in turn leads to higher involvement of the EDPB, has had a significant impact on the workload. The success in the performance of these tasks relies largely on the resources available to the DPAs and to the EDPB, including via its Secretariat.

Most DPAs (21) explicitly stated that their allocated budget was not sufficient for carrying out their activities, while other DPAs considered they had sufficient financial resources. Based on information provided by 28 DPAs from EEA countries, some DPAs have barely seen a budgetary increase between 2020 and 2024, and one DPA (EL) saw a budgetary decrease.

In terms of human resources, the vast majority of DPAs (25) stated that current staffing is not sufficient to face their workload. 7 DPAs still have the same number of staff members in 2023 as in 2022, despite the increasing workload.

4.2. GENERAL GUIDANCE ADOPTED IN 2023

General guidance drafted in 2023 before public consultation

- Guidelines 01/2023 on Article 37 Law Enforcement Directive, adopted: 19 September 2023;
- Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, adopted: 14 November 2023.

General guidance adopted in 2023 after public consultation

- Guidelines 03/2021 on the application of Article 65(1)(a) GDPR, adopted: 24 May 2023;
- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, adopted: 14 February 2023;
- Guidelines 01/2022 on data subject rights - Right of access, adopted: 28 March 2023;

- Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, adopted: 14 February 2023;
- Guidelines 04/2022 on the calculation of administrative fines under the GDPR, adopted: 24 May 2023;
- Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted: 26 April 2023;
- Guidelines 07/2022 on certification as a tool for transfers, adopted: 14 February 2023;
- Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority, adopted: 28 March 2023;
- Guidelines 9/2022 on personal data breach notification under GDPR, adopted: 28 March 2023;
- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted: 20 June 2023.

4.3. BINDING DECISIONS ADOPTED IN 2023

- Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR), adopted: 27 October 2023;
- Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), adopted: 13 April 2023;
- Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), adopted: 2 August 2023.

4.4. CONSISTENCY OPINIONS ADOPTED IN 2023

Opinions on DPA's approval of accreditation requirements for a code of conduct monitoring body

- Opinion 1/2023 on the draft decision of the competent supervisory authority of Croatia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Article 41 GDPR, adopted: 3 February 2023;
- Opinion 02/2023 on the draft decision of the competent supervisory authority of Latvia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Article 41 GDPR, adopted: 3 February 2023;
- Opinion 03/2023 on the draft decision of the competent supervisory authority of Romania regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR, adopted: 3 February 2023;
- Opinion 11/2023 on the draft decision of the competent supervisory authority of Sweden regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR, adopted: 11 July 2023.

Opinions on draft requirements for the accreditation of a certification body

- Opinion 4/2023 on the draft decision of the competent supervisory authority of Malta regarding the approval of the requirements for

accreditation of a certification body pursuant to Article 43.3 (GDPR), adopted: 3 February 2023;

- Opinion 12/2023 on the draft decision of the competent supervisory authority of Cyprus regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR), adopted: 11 July 2023;
- Opinion 13/2023 on the draft decision of the competent supervisory authority of Croatia regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR), adopted: 11 July 2023;
- Opinion 37/2023 on the draft decision of the competent supervisory authority of Luxemburg regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR), adopted: 21 December 2023;
- Opinion 38/2023 on the draft decision of the competent supervisory authority of Slovenian regarding the approval of the requirements for accreditation of a certification body pursuant to Art 43.3 (GDPR), adopted: 21 December 2023.

Opinions on draft decisions regarding Binding Corporate Rules

- Opinion 6/2023 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Royal Greenland Group, adopted: 23 March 2023;
- Opinion 7/2023 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Autodesk Group, adopted: 5 May 2023;
- Opinion 8/2023 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of Autodesk Group, adopted: 5 May 2023;
- Opinion 9/2023 on the draft decision of the Italian Supervisory Authority regarding the Controller Binding Corporate Rules of Vertiv, adopted: 17 May 2023;
- Opinion 10/2023 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the PROSEGUR Group, adopted: 30 June 2023;
- Opinion 14/2023 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Vestas Wind Systems Group, adopted: 27 July 2023;
- Opinion 16/2023 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Informatica Group, adopted: 28 September 2023;
- Opinion 17/2023 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Informatica Group, adopted: 28 September 2023;
- Opinion 18/2023 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of the Collibra Group, adopted: 7 November 2023;
- Opinion 19/2023 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the American Express Global Business Travel Group, adopted: 16 November 2023;

- Opinion 20/2023 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the Comcast Corporation Group, adopted: 16 November 2023;
- Opinion 21/2023 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of the UPS Group, adopted: 16 November 2023;
- Opinion 22/2023 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules for employee data of the UPS Group, adopted: 16 November 2023;
- Opinion 23/2023 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules for customer data of the UPS Group, adopted: 16 November 2023;
- Opinion 24/2023 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Nestlé Group, adopted: 16 November 2023;
- Opinion 25/2023 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the SHV Holding N.V. Group, adopted: 16 November 2023;
- Opinion 26/2023 on the draft decision of the Romanian Supervisory Authority regarding the Processor Binding Corporate Rules of the OSF Global Services Group, adopted: 16 October 2023;
- Opinion 27/2023 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the Tessi Group, adopted: 28 November 2023;
- Opinion 28/2023 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Servier Group, adopted: 28 November 2023;
- Opinion 29/2023 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Sodexo Group, adopted: 28 November 2023;
- Opinion 30/2023 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the Sodexo Group, adopted: 28 November 2023;
- Opinion 31/2023 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Thalès Group, adopted: 28 November 2023;
- Opinion 32/2023 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the Thalès Group, adopted: 28 November 2023;
- Opinion 33/2023 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Controller Binding Corporate Rules of the Cerner Group, adopted: 13 December 2023;
- Opinion 34/2023 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Processor Binding Corporate Rules of the Cerner Group, adopted: 13 December 2023;
- Opinion 35/2023 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Carlsberg Group, adopted: 13 December 2023;
- Opinion 36/2023 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the

Booking.com Group, adopted: 28 December 2023.

Opinions on certification criteria

- Opinion 15/2023 on the draft decision of the Dutch Supervisory Authority regarding the Brand Compliance certification criteria, adopted: 19 September 2023.

4.5. CONSULTATIONS RELATING TO LEGISLATION AND TO DRAFT ADEQUACY DECISIONS

- EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, adopted: 19 September 2023;
- Joint EDPB-EDPS contribution to the public consultation on the draft template relating to the description of consumer profiling techniques (Art.15 DMA), adopted: 20 September 2023;
- EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, adopted: 17 October 2023;
- Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, adopted: 28 February 2023.

4.6. OTHER DOCUMENTS

Engagement and awareness raising

- Data Protection Guide for Small Business.

Coordinated Enforcement Framework

- Coordinated Enforcement Action, use of cloud-based services by the public sector.

International cooperation

- Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023;
- Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan.

Organisational nature

- EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals;
- EDPB Work Programme 2023-2024.

Support to enforcement activities

- Report of the work undertaken by the Cookie Banner Taskforce;
- Report of the work undertaken by the supervisory authorities within the 101 Task Force;
- Template Complaint form and Template Acknowledgement of receipt.

CONTACT DETAILS

Postal address

Rue Wiertz 60, B-1047 Brussels

Office address

Rue Montoyer 30, B-1000 Brussels

edpb
European Data Protection Board

An Executive Summary of this report, which provides an overview of key EDPB activities in 2023, is also available. Further details about the EDPB can be found on our website at edpb.europa.eu.