edpb
European Data Protection Board

ANNUAL REPORT 2024

PROTECTING PERSONAL DATA IN A CHANGING LANDSCAPE

TABLE OF CONTENTS

FOREWORD

It is with great pleasure that I present the European Data Protection Board's (EDPB) 2024 annual report. Reading this report, you will learn about the milestones the EDPB achieved in 2024, a year during which the Board has shown, once more, its commitment to upholding the fundamental right of privacy and data protection.

In April 2024, we adopted our new strategy 2024-2027. The strategy outlines key priorities and actions to strengthen data protection, ensure consistent enforcement of the GDPR, and address emerging challenges in a rapidly evolving digital landscape. It will help us further strengthen, modernise and harmonise data protection across Europe via four main pillars and a series of key actions.

In 2024, we have also continued to provide guidance and legal advice. Remarkably, we did not issue any Art. 65 binding decisions in the past year, whilst we have observed a sharp increase in the number of requests for opinion on questions of general application, under Art. 64(2). For example, we adopted an opinion on the validity of 'Consent or Pay' models deployed by large online platforms. The models we have today usually require individuals to either give away their data or to pay. As a result, most users consent to the processing in order to use a service, and they do not understand the full implications of their choices. According to our opinion, large online platforms will, in most cases, not be able to comply with the requirements for valid consent if they confront users only with a choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee.

Art. 64(2) opinions are an important tool allowing for consistency from an early stage and several more of these opinions were adopted in 2024, including on the notion of main establishment, the use facial recognition at airports, the reliance on processors and sub-processors, and the use of personal data to train AI models.

With this last opinion, the EDPB aims to support responsible AI innovation by ensuring personal data used to train AI models are protected and in full respect of the General Data Protection Regulation (GDPR).

AI technologies may bring many opportunities and benefits to different industries and areas of life, and we need to ensure these innovations are done ethically, safely, and in a way that benefits everyone. In our opinion, we confirm AI developers can use legitimate interest as a legal basis for model training, under certain conditions. To help developers determine if they are using it lawfully, the EDPB put forward a three-step test.

New digital legislations, including the Digital Markets Act (DMA), the Digital Services Act (DSA), the AI Act, the Governance Act and the Data Act, have come into force recently. These legislations address a variety of important issues, and all of them are built on the foundation laid by the GDPR. Increasingly, we will find that fairness, contestability, and the protection of fundamental rights will need to be approached from multiple regulatory angles. This requires seamless cross-regulatory collaboration and the EDPB will actively contribute to it.

As we move into this new phase, the number of formal regulatory roles of the EDPB and Data Protection Authorities (DPAs) are expanding. On top of that, the EDPB already pro-actively seeks the input of other regulators. For example, the EDPB met with the EU AI Office and took on board its views prior to adopting the opinion on AI Models.

Finally, the EDPB continued its efforts to provide information on the GDPR to a broad audience, presenting it in clear, non-technical language. To this end, our Data Protection Guide for Small Business, previously launched in 2023, was made available in 18 languages in 2024. In addition, we launched a series of summaries of EDPB guidelines to help non-expert individuals and organisations identify in an easier way the most important points to consider.

Chairing the EDPB over the last two years has been a true privilege, and I am confident that the work of the DPAs and the EDPB Secretariat will continue to strengthen data protection and privacy in the years to come.

Anu Talus

Chair of the European Data Protection Board

HIGHLIGHTS

2024

JANUARY

Coordinated Enforcement report on the role of DPOs

FEBRUARY

- Launch Coordinated Enforcement action on the right of access
- Opinion 04/2024 on the notion of main establishment of a controller

APRIL

- Opinion 08/2024 on 'Consent or Pay' models deployed by large online platforms
- Adoption 2024-2027 Strategy

MAY

Opinion 11/2024 on the use of facial recognition technologies to streamline airport passengers' flow

JUNE

Election of a new EDPB Deputy Chair Zdravko Vukić

OCTOBER

- Guidelines on Legitimate Interest and first meeting of EDPB with DPAs of countries with an adequacy decision
- Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)

NOVEMBER

Stakeholder events on AI models and "Consent or Pay"

DECEMBER

Opinion 28/2024 on AI models

1. THE EDPB SECRETARIAT

Reflecting on the work accomplished in 2024, we observe that the number of responsibilities of the EDPB has increased and that this has an impact on the work done by the EDPB Secretariat.

As we transitioned into a new regulatory digital framework [1], the EDPB proved ready to take on new roles, for example by becoming a member of the DMA High-Level Group, of the European Data Innovation Board (EDIB) or by cooperating with the European Board for Digital Services (EBDS). In 2024, the EDPB also cooperated with competition and consumer authorities and the AI office. This cross-regulatory cooperation as well as the launch of the work on several guidelines on the interplay between the GDPR and other digital regulations are part of the new EDPB Strategy 2024-2027.

While it is the first year since 2020 that the EDPB did not adopt any binding decision, we saw an important increase of request for consistency opinions under Art. 64(2) GDPR.

These opinions deal with a matter of general application or producing effects in more than one Member State and have proven to be a crucial tool for the consistent application of the GDPR by Data Protection Authorities (DPAs) in the context of new technologies.

In 2024, the EDPB Secretariat organised two stakeholder events on topics having an important societal relevance, such as the use of personal data to train AI models and "Consent or Pay" mechanisms used for behavioural advertising. We hosted these events not only because we are committed to transparency, but also because we consider stakeholders' input essential for the quality of our work.

In order to ensure that our guidance is accessible for non-experts, individuals (including children), and SMEs, we started to develop information sheets to share guidelines' core messages.

[1] New digital legislations, including the Digital Markets Act (DMA), the Digital Services Act (DSA), the AI Act, the Governance Act and the Data Act.

This is a new activity in the same spirit as the Data Protection Guide for Small Business that we developed in 2023.

Another area of growth in 2024 was the support the EDPB Secretariat offers to the Coordinated Supervisory Committee (CSC), which ensures coordinated supervision of large scale IT systems and EU bodies and agencies. In 2024, the activity of the CSC was extended to the supervision of the Visa Information System (VIS), in addition to the Schengen Information System (SIS), Europol, the EPPO, Eurojust and IMI that were already falling under the framework of the EDPB activities. Substantial work has been dedicated to the preparation of the supervision of ETIAS. In the near future, the interoperability will interconnect seven EU-information systems, three existing systems (SIS, VIS, Eurodac and PrümII) and three new systems, yet to be set up (EES, ETIAS and ECRIS-TCN).

The increased activities of the Board led to a significant surge in the support the EDPB Secretariat offers to EDPB members. As figures sometimes speak louder than words, I believe it is important to mention that the EDPB Secretariat organised over 530 meetings in 2024 (up from over 360 in 2023) and managed over 4.200 requests for IT assistance and queries from our members (up from 3.400 in 2023).

To ensure that the EDPB Secretariat can continue to successfully perform its tasks and accomplish its mission, it is essential to get the appropriate resources in terms of staff and budget.

I would like to thank the EDPB Secretariat's staff and the Board's members who contributed to each single achievement we reached throughout 2024. This is a testament to the dedication of each of us, our steady cooperation and our commitment to ensuring the EDPB's daily operations run smoothly and effectively.

The work of the Secretariat will continue to evolve to meet the changing needs of the evolving technological and regulatory landscape, and together we stay strong in our commitment to further uphold the right of data protection across Europe and beyond in the years ahead.

Isabelle Vereecken

Head of the EDPB Secretariat

1.1 MISSION AND ACTIVITIES

The European Data Protection Board (EDPB) Secretariat offers analytical, administrative and logistical support to the Board. Its overarching mission is to ensure that the EDPB functions effectively, facilitating the adoption of binding decisions, legal opinions, consistency opinions and guidance under the General Data Protection Regulation (GDPR). Beyond its core legal work, the Secretariat acts as a vital communication channel, ensuring a cohesive and consistent approach to data protection across Europe.

The EDPB Secretariat assists the EDPB Members in enforcing data protection laws by fostering consistency and promoting cooperation among Data Protection Authorities (DPAs). For a limited number of complex cases where DPAs cannot reach a consensus, the EDPB issues binding decisions. As a neutral party among DPAs, the Secretariat provides essential support in drafting these decisions, ensuring impartiality and adherence to regulatory standards.

In 2024, the Secretariat's work reflected the growing complexity and breadth of the GDPR implementation. The Secretariat was instrumental in drafting eight consistency opinions under Art. 64(2) GDPR, which provide guidance to national DPAs on any matter of general application or producing effects in more than one Member State. Any DPA, the Chair of the Board, or the European Commission may request such opinions, particularly in cases where a competent national authority is deemed not to fulfil its obligations regarding mutual assistance. These opinions provided authoritative guidance on cross-border data protection measures, addressing challenges unique to a rapidly evolving digital landscape. For instance, one consistency opinion focused on the processing of facial recognition to streamline airport passengers' flow, a subject of increasing importance as digital authentication methods evolve.

Furthermore, the Secretariat oversaw significant litigation activities, representing the EDPB as a party in multiple cases before the Court of Justice of the European Union (CJEU).

In 2024, the EDPB was involved as a main party in 13 cases before the CJEU, one of which was submitted in 2022,[2] ten in 2023,[3] and two in 2024.[4] Most of the cases concerned applications for annulment against binding decisions adopted by the EDPB. The two cases submitted in 2024 concerned applications for annulment against an urgent binding decision and against an opinion. In addition, in 2024 the EDPB was involved as intervener in one case, in support of the European Data Protection Supervisor (EDPS). During all these proceedings, the Secretariat of the EDPB collaborated closely with external lawyers at every stage. This included defining the EDPB's legal strategy, drafting procedural documents, and preparing for and attending hearings before the CJEU.

"The EDPB is a dynamic and collaborative body that plays a pivotal role in ensuring the consistent application of data protection laws across Europe. From my perspective as Deputy Chair, I see it as a guardian of individuals' privacy rights, skilfully balancing the needs of innovation and economic growth. Our diverse membership strengthens our ability to address complex data protection issues and fosters a culture of shared responsibility among member states."

Zdravko Vukić
Director of the Croatian Personal Data Protection Agency and EDPB Deputy Chair

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 European Union 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.

Budget management remained a priority in 2024. The EDPB budget forms part of the broader budget of the EDPS. Operating within an approved budget of €8.36 million, the Secretariat effectively allocated resources to support enforcement, litigation, and operational activities.

Operational structure

The EDPB Secretariat has evolved into a robust and dynamic organisation. It comprises a team of 39[5] highly specialised professionals dedicated to supporting the Board's activities. Organised into five distinct sectors focusing on legal affairs, litigation and international affairs, IT matters, information and communications, and administrative matters, the Secretariat ensures that all aspects of the EDPB's mandate are addressed comprehensively.

While formally employed by the EDPS, the Secretariat staff operate under the exclusive direction of the EDPB Chair. The cooperation framework between the EDPB and the EDPS is defined by a Memorandum of Understanding. This structure facilitates seamless collaboration and ensures that the Secretariat can fully dedicate its resources to supporting the Board's work. In 2024, the Secretariat prioritised staff development, introducing targeted training programs on emerging technologies such as AI to better address future challenges in data protection.

[2] Case T-682/22 Meta Platforms Ireland v EDPB.
[3] Cases 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.
[4] Case T-8/24 Meta Platforms Ireland v EDBP and Case T-319/24 Meta Platforms Ireland v EDPB.
[5] The EDPB budget covers 46 posts, including seven posts at the EDPS for the support provided to the EDPB via horizontal administrative services.

Data protection and transparency

The EDPB Secretariat is also responsible for handling Access to Documents (AtD) requests, in accordance with Art. 32(2) of the EDPB Rules of Procedure (RoP). These activities ensure transparency and accountability in the Board's operations by facilitating public access to the EDPB documents.

Initial AtD requests are handled and signed by one of the Deputy Chairs. Confirmatory requests are handled and signed by the Chair. In 2024, the EDPB received 38 access requests for documents held by the EDPB. Confirmatory applications were received in three cases. No complaint regarding the EDPB confirmatory decisions for a request for access to documents was brought to the attention of the European Ombudsman in 2024.

The EDPB processes personal data according to the rules laid down in Regulation (EU) 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 Data Protection Officer (DPO) team, which is part of the EDPB Secretariat. In 2024, the EDPB received 18 individual requests based on rights enshrined in Art. 17 to Art. 24 of Regulation (EU) 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 six data breaches under Arts. 34 and 35 of Regulation (EU) 2018/1725, one of which required a notification to the EDPS.

IT systems

In 2024, the EDPB Secretariat achieved significant advancements in its IT systems, continuing to enhance cooperation and communication among DPAs. The Internal Market Information (IMI) system remained a fundamental part of the GDPR cooperation, facilitating over 5.644 procedures during the

The Secretariat handled 907 support requests related to the IMI system and managed a total of 4.225 inquiries across all the EDPB IT systems, ensuring timely and effective assistance for all stakeholders.

In addition, the EDPB Secretariat introduced a centralised training resource to improve the accessibility and effectiveness of its IT tools. This hub offers detailed guidance on how information is structured within the primary EDPB information exchange platform and provides various user guide materials for using the various EDPB IT systems. Furthermore, the EDPB Secretariat developed a comprehensive series of videos showcasing the key features of these IT systems, further promoting efficient collaboration.

The EDPB HUB, the primary platform for internal communication and information sharing, experienced significant growth in 2024. Over 12.307 content pieces were created and shared, reflecting a substantial 64% increase compared to the previous year. This included 2.372 new pages, making a 59% rise, and 8.217 documents, which represents 72% growth. Exchanges also increased, reaching 1.389, a 37% more over 2023, alongside 329 other types of content. With a user base now exceeding 1.500 Members (a 7% increase) the platform continues to be a vital tool for collaboration and innovation.

The Secretariat also ensured the uninterrupted operation of the EDPB website, which received 329.432 visits over the course of the year. The most frequently accessed sections included Guidelines, Recommendations, Best Practices, Documents, Opinions, the Cookie Policy, Career opportunities, Binding Decisions, Contact us and News.

These digital platforms continue to play a critical role in advancing the EDPB's mission and enhancing its operational efficiency.

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 2024

"The year 2024 has once again confirmed the importance of cooperation between European data protection authorities in responding to the concerns of individuals and, where necessary, punishing breaches of the regulations. Faced with the major technological and societal challenges of today, particularly those relating to artificial intelligence, cybersecurity and the rights of minors, it is more necessary than ever to strengthen our synergies and harmonise our practices."

Marie-Laure Denis
Head of French Data Protection Authority

2024-2027 Strategy and 2024-2025 Work Programme

In 2024, the EDPB remains steadfast in its mission to consistent application of data protection laws across Europe while fostering stronger collaboration among DPAs. The 2024-2027 Strategy and the 2024-2025 Work Programme provide a comprehensive roadmap to address emerging challenges, safeguard fundamental rights, and adapt to the rapid evolution of digital technologies.

Structured around four key pillars, the 2024-2027 Strategy guides the EDPB's actions and priorities:

- **Pillar 1 on advancing harmonisation and promoting compliance** aims at ensuring consistent and effective application of data protection laws across countries;
- **Pillar 2 on reinforcing a common enforcement culture** aims at strengthening collaboration among DPAs to address complex cases and enhance cross-border cooperation;
- **Pillar 3 on addressing technological challenges** aims at emphasising a human-centric approach to emerging technologies, safeguarding fundamental rights, and navigating an evolving regulatory landscape;

- **Pillar 4 on enhancing the EDPB's global role** aims at engaging with international partners to promote high data protection standards worldwide.

The 2024-2025 Work Programme is the first of two which will implement the EDPB Strategy for 2024–2027. It is based on the priorities set out in the EDPB Strategy.

The Work Programme lists several key actions, which serve to implement the EDPB Strategy. These include:

- Providing concise, practical and clear guidance that is accessible to the relevant audience, as well as tools and content for a non-expert audience, including particularly vulnerable data subjects such as children;
- Supporting the development of compliance measures and engagement with stakeholders;
- Strengthening efforts to ensure effective enforcement of the GDPR and cooperation between the Members of the EDPB, building on its commitments made in the Vienna Statement on enforcement cooperation and on the opportunities arising from the future Regulation on the GDPR procedural rules;
- Establishing common positions and guidance in the cross-regulatory landscape and cooperating with other regulatory authorities on matters relating to data protection, including competition authorities, consumer protection authorities and authorities competent under other legal acts;
- Monitoring and assessing new technologies;
- Promoting a global dialogue on privacy and data protection, including a focus on the international community, and supporting cooperation on enforcement between EU and non-EU authorities.

New roles and responsibilities in a changing environment

In response to the unprecedented pace of technological advancement, the EU implemented a series of digital laws in 2024. These regulations have expanded the responsibilities of DPAs, giving them new roles in overseeing compliance and safeguarding data protection.

The AI Act designates DPAs (or other authorities with the same requirements on independence) as Market Surveillance Authorities (MSA) for certain high-risk AI systems, reinforcing their central role in protecting data protection rights.

Similarly, under the Data Act, DPAs ensure personal data processing aligns with the GDPR standards, supported by enhanced cooperation frameworks to manage new regulatory demands.

As a Member of the High-Level Group on the Digital Markets Act (DMA), the EDPB provided critical guidance to the European Commission, fostering a cohesive and harmonised regulatory approach across data governance frameworks. This collaboration ensured alignment between data protection law and sectoral regulations, reflecting the interconnected nature of digital governance.

The EDPB also actively participated in the European Board for Digital Services, addressing critical issues within the internal market. Its efforts included supporting the oversight of large online platforms and search engines and contributing to the Age Verification Taskforce. As a Member of the European Data Innovation Board, the EDPB played a pivotal role in initiatives related to data sharing and the development of European data spaces. These responsibilities align with the Board's broader mission to address complex, cross-border and cross-regulatory challenges in the digital era.

"The European Data Protection Board (EDPB) drives global privacy standards by ensuring consistent GDPR application, fostering transparency and trust. In the world of new technologies, the EDPB will play a crucial role in guiding innovation while protecting privacy, strengthening international cooperation, and addressing emerging challenges in the digital environment."

Dijana Šinkūnienė
Director of the State Data Protection Inspectorate of the Republic of Lithuania

"Cooperation through EDPB is one of my priorities as the new Slovenian Information Commissioner. Data protection in the EU would undoubtedly be much weaker without the EDPB and GDPR. Especially with the challenges brought by the digital landscapes and the new duties the DPAs will be having in the AI regulatory framework."

Dr. Jelena Virant Burnik
Information Commissioner of the Republic of Slovenia

2.1 CONSISTENCY OPINIONS

Consistency opinions are a driving force of the EDPB's mission to ensure the uniform interpretation and application of the GDPR across the EU. Established under Art. 64 GDPR, these opinions provide authoritative, non-binding recommendations that align DPAs decisions with a common EU framework. By addressing areas of potential divergence, consistency opinions contribute to harmonised enforcement and legal clarity.

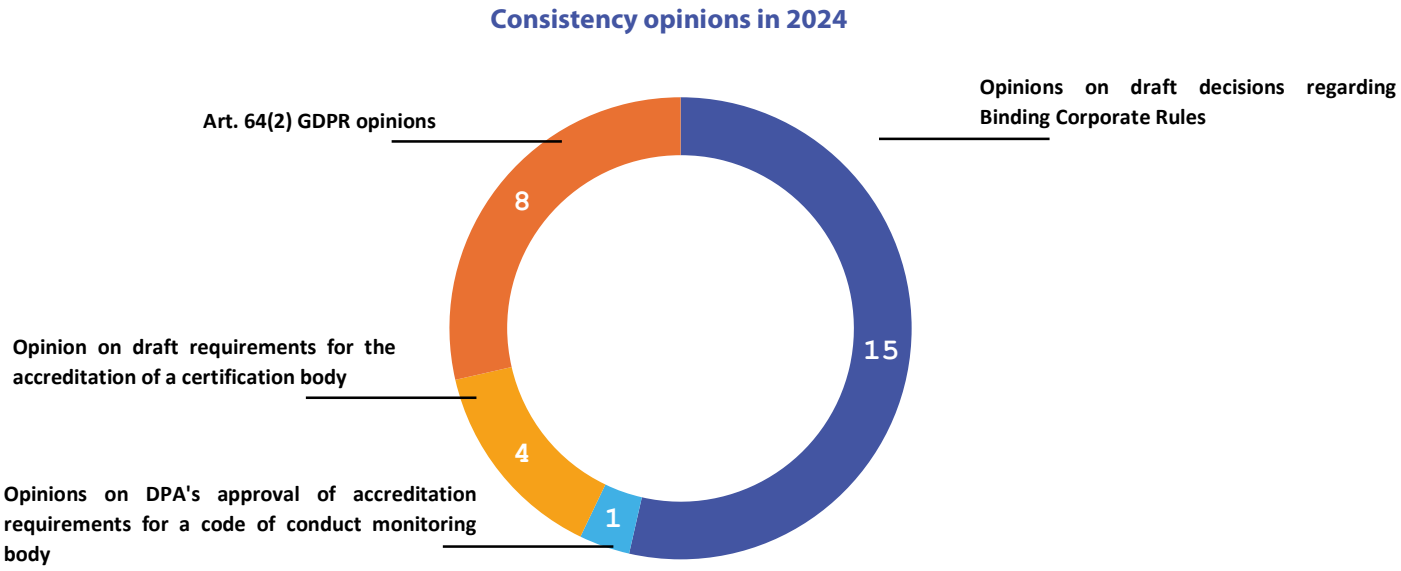
DPAs may request a consistency opinion from the EDPB when considering measures that could impact multiple jurisdictions. Once issued, these opinions serve as guiding documents, enabling DPAs to finalise their decisions while ensuring alignment with the GDPR standards. In 2024, 28 opinions were issued under two distinct mechanisms: Art. 64(1) GDPR and Art. 64(2) GDPR, each addressing specific regulatory needs and challenges.

2.1.1 Art. 64(1) GDPR Opinions

Art. 64(1) GDPR mandates the issuance of consistency opinions for specific measures that DPAs intend to adopt. These opinions are pivotal in ensuring the uniform application of the GDPR provisions and fostering regulatory coherence across countries. The six categories of measures requiring consistency opinions under Art. 64(1) GDPR include:

- Lists of processing operations requiring Data Protection Impact Assessments (DPIAs): these lists identify activities that are likely to pose significant risks to individuals' rights and freedoms;
- Draft codes of conduct: tailored to specific sectors or processing activities, these codes facilitate compliance by providing industry-specific guidance while ensuring alignment with the GDPR principles;
- Accreditation of certification bodies, of criteria for certification bodies, and schemes: these criteria establish the standards for certification, promoting trust and accountability in data protection;
- Draft decisions on standard contractual clauses (SCC) for international data transfers: these clauses provide legally robust mechanisms for transferring personal data outside the EU, ensuring continuity in data protection;
- Authorisations for custom contractual clauses: bespoke clauses tailored to specific circumstances, requiring the EDPB review to ensure compliance with the GDPR requirements;
- Approvals of Binding Corporate Rules (BCRs): these rules govern intra-group data transfers within multinational organisations, ensuring consistent application of the GDPR principles across jurisdictions.

In 2024, the EDPB adopted 20 Art. 64(1) GDPR opinions, reflecting its continued commitment to promoting harmonisation. Since its establishment in 2018, the EDPB has issued a total of 188 Art. 64(1) opinions, demonstrating the sustained importance of this mechanism in supporting a harmonised application of the GDPR. ***See Section 4.2.1 for the complete list of opinions adopted in 2024.***



2.1.2 Art. 64(2) GDPR Opinions

Art. 64(2) GDPR provides a mechanism for the EDPB to issue consistency opinions on matters of general application or those with significant cross-border implications. Such opinions can be requested by the EDPB Chair, DPAs, or the European Commission to address broad, recurring issues or complex legal questions, ensuring alignment across Member States. These opinions help avoid conflicting DPAs decisions and ensure that the GDPR rules are applied consistently in the EU.

In 2024, the EDPB adopted eight Art. 64(2) GDPR opinions, highlighting the growing importance of this mechanism in addressing critical data protection challenges. ***See Section 4.2.2 for the complete list of opinions adopted in 2024.***

2.1.2.1 Opinion 4/2024 on the notion of main establishment of a controller in the Union under Article 4(16)(a) GDPR

In February 2024, the EDPB issued Opinion 4/2024 following a request by the French DPA to clarify the notion of "main establishment" of a data controller in the Union pursuant to Art. 4(16)(a) GDPR.

Scope of the Opinion

The notion of "main establishment" is pivotal in determining the lead DPA responsible for overseeing a data controller's compliance with the GDPR and has therefore important consequences for the practical application of the one-stop-shop mechanism.

In its request to the Board, the French DPA asked whether:

- For a data controller's "place of central administration in the Union" to be qualified as a main establishment under Art. 4(16)(a) GDPR, this establishment should take decisions on the purposes and means of the processing and have the power to have them implemented;
- The one-stop-shop mechanism applies only if there is evidence that one of the establishments in the Union of the data controller (the data controller's "place of central administration" or not) takes the decisions on the purposes and means concerning the processing operations in question and has the power to have such decisions implemented.

Key considerations

Based on Art. 4(16)(a) GDPR, the EDPB determined that a "place of central administration" in the EU should be considered the main establishment only if it makes decisions regarding the purposes and means of personal data processing and has the authority to implement those decisions.

The EDPB further explained that the one-stop-shop mechanism can only apply if there is evidence that one of the establishments of the data controller in the Union takes decisions on the purposes and means for the relevant processing operations and has the power to have these decisions implemented. This means that, when the

decisions on the purposes and means of the processing are taken outside of the EU, there should be no main establishment of the data controller in the Union, and therefore the one-stop-shop should not apply.

Practical implications and recommendations

The EDPB provided useful clarifications on how the DPAs should apply in practice Art. 4(16)(a) GDPR to ensure its uniform application. In particular, the EDPB recalled that the burden of proof in relation to the place where the relevant processing decisions are taken and where there is the power to implement such decisions in the Union ultimately falls on data controllers.

In addition, the DPAs retain the ability to challenge the data controller's claim based on an objective examination of the relevant facts, requesting further information where required. The EDPB further stated that when determining the location of the data controller's main establishment, DPAs should duly cooperate and jointly agree, depending on the concrete case, on the level of detail the data controller should provide.

2.1.2.2 Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms

In April 2024, the EDPB adopted Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, following a request from the Dutch, Norwegian, and German (Hamburg) DPAs. This Opinion addresses whether consent, as defined under Art. 4 (11) GDPR, is valid and, in particular, "freely given", when users face a stark choice between allowing data processing for behavioural advertising or paying a fee for an alternative service.

Acknowledging the cross-regulatory implications, the EDPB collaborated with national and EU-level competition and consumer protection regulators to integrate broader perspectives into its assessment. This cooperation has proven very useful in providing valuable input for the Opinion on Consent or Pay.

Scope of the Opinion

The scope of this Opinion is limited to the use of "Consent or Pay" models by large online platforms, defined by their significant reach and influence over millions of users across the EU. These platforms often leverage behavioural advertising as a primary revenue stream, offering services where users are asked either to consent to the processing of their personal data for advertising purposes or to pay a fee to access an ad-free or data-minimised version of the service. The Opinion draws on the GDPR and relevant case law, particularly the July 2023 ruling by the Court of Justice of the European Union (CJEU) in the Bundeskartellamt case (C-252/21), which addressed issues of consent and power imbalance in the context of large online platforms.

Key considerations

The EDPB reiterated several core principles of the GDPR in its assessment, particularly:

- **Necessity and proportionality**: processing personal data for behavioural advertising must be proportionate to the purpose and limited to what is strictly necessary. The "Consent or Pay" models, as commonly implemented, often fail to meet these standards;
- **Fairness and accountability**: data controllers must ensure that users fully understand the implications of consenting to data processing. The Board emphasised the importance of fairness in offering a real choice without undue pressure or coercion. Data controllers must also document how consent is obtained and ensure they can demonstrate compliance with the GDPR's accountability principle;
- **Granularity and transparency**: consent must be specific and granular. Users should be able to consent to purposes for data processing without being forced into a bundled consent covering multiple, distinct purposes. Platforms must clearly explain each option and its implications in accessible and plain language;
- **Conditionality**: consent is presumed not to be freely given if it is conditional on accessing a service where processing is not necessary for the provision of that service. Platforms that offer only two stark choices – consenting to intrusive behavioural advertising or paying a fee – may fail to provide a true alternative and may undermine the principle of free consent.

The challenges of "Consent or Pay" models

The Board recognised that "Consent or Pay" models by large online platforms often do not satisfy the GDPR's requirement that consent must be freely given. Many users feel pressured to consent to data processing rather than pay, particularly when services are part of individuals' daily lives, or essential to social interactions, or professional networking. The Opinion further elaborates on the risks of these models, identifying three primary issues:

- **Imbalance of power**: in many cases, large online platforms hold a dominant market position, limiting users' ability to reject consent without significant detriment. The CJEU Bundeskartellamt case underlined that a platform's dominant position could hinder users from refusing consent, as their ability to choose an alternative service is often limited or non-existent;
- **Detriment to users**: the EDPB stressed that consent cannot be considered freely given if the user suffers detriment for refusing. For instance, if users are excluded from accessing important services or social interactions due to non-consent, this would undermine the validity of their choice. The financial burden of paying for an ad-free version can also be seen as a detriment, particularly when the fee is prohibitively high;
- **Lack of genuine alternatives**: to provide a real choice, the EDPB emphasised the importance of offering an "equivalent alternative" that does not require either payment or extensive personal data collection. For example, platforms could offer a version with non-personalised advertising, where only minimal and non-behavioural data is collected. Providing this type of alternative helps mitigate concerns about the validity of consent.

Recommendations for DPAs

The EDPB made considerations for DPAs to take into account when large online platforms seek to comply with the GDPR when implementing "Consent or Pay" models:

- **Offer a free alternative without behavioural advertising**: platforms should consider providing a version of their service that does not rely on behavioural advertising but instead uses less intrusive forms of advertising, such as contextual ads based on the content viewed. This would allow users to enjoy the service without the need to consent to invasive data processing or pay a fee. DPAs should also consider more generally if consent is freely given, if there is an imbalance of power and if the individual would suffer detriment as a consequence of not consenting. Consent should also be specific;
- **Transparency and information**: users must be fully informed about the consequences of their choices. The EDPB considers that platforms should adopt clear and simple communication to ensure users understand what data is collected, how it is used, and what opting out or paying entails;
- **Avoiding high fees**: any fee charged for accessing a service without behavioural advertising should be proportionate and must not discourage users from exercising their right to refuse consent. Excessive fees that compel users to consent instead of paying for the alternative are not acceptable under the GDPR.

The EDPB concluded that most current implementations of "Consent or Pay" models by large online platforms are unlikely to meet the GDPR's strict requirements for valid consent. To this end, the EDPB will also be developing further guidelines on the use of 'Consent or Pay' models, with a broader scope and stakeholder engagement.

This Opinion marks a significant step in addressing the growing concerns over the use of personal data by large online platforms and the ways in which users' consent is obtained. The EDPB remains committed to ensuring that the fundamental right to data protection is upheld, especially in the face of increasingly complex business models that seek to monetise personal data.

2.1.2.3 Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow

In May 2024, the EDPB issued Opinion 11/2024 on the use of facial recognition technologies by airports and airlines to streamline passengers' flow.

Scope of the opinion

The French DPA requested this Opinion due to increasing deployment of biometric systems at major airports across the EU, raising significant data protection concerns. The EDPB's role was to ensure that such systems comply with the GDPR principles while safeguarding individuals' fundamental rights to privacy and data protection.

Key considerations

Facial recognition technologies are often promoted as tools to enhance efficiency and convenience in the travel industry. However, these systems also involve the processing of sensitive biometric data, necessitating compliance with Art. 5(1)(e) GDPR, Art. 5(1)(f) GDPR, Art. 25 GDPR, and Art. 32 GDPR, among others.

There is no uniform legal requirement in the EU for airport operators and airline companies to verify that the name on the passenger's boarding pass matches the name on their identity document, and this may be subject to national laws. Therefore, where no verification of the passengers' identity with an official identity document is required, no such verification with the use of biometrics should be performed, as this would result in an excessive processing of data.

Different storage solutions and their implications

In its Opinion, the EDPB considered the compliance of processing of passengers' biometric data with four different types of storage solutions, ranging from ones that store the biometric data only in the hands of the individual to those which rely on a centralised storage architecture with different modalities. In all cases, only the biometric data of passengers who actively enrol and consent to participate should be processed.

The EDPB found that the only storage solutions which could be compatible with the integrity and confidentiality principle, data protection by design and default and security of processing, are the solutions whereby the biometric data is stored in the hands of the individual or in a central database but with the encryption key solely in their hands. These storage solutions, if implemented with a list of recommended minimum safeguards, are the only modalities which adequately counterbalance the intrusiveness of the processing by offering individuals the greatest control. The EDPB found that the solutions that were examined and which are based on the storage in a centralised database either within the airport or in the cloud, without the encryption keys in the hands of the individual, cannot be compatible with the requirements of data protection by design and default and, if the data controller limits themselves to the measures described in the scenarios analysed, would not comply with the requirements of security of processing.

2.1.2.4 Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)

In October 2024, the EDPB adopted Opinion 22/2024 concerning certain obligations of data controllers when engaging data processors and sub-processors, stemming from the requirements of Art. 28 GDPR and in light of the principle of accountability. This Opinion was requested by the Danish DPA.

Scope of the Opinion

The Opinion is about situations where controllers rely on one or more processors and sub-processors. In particular, it addresses questions on the interpretation of certain duties of controllers in such a situation, as well as the wording of controller-processor contracts. The questions address processing of personal data in the European Economic Area (EEA) as well as processing following a transfer to a third country.

Key considerations

The Opinion explains that controllers should have the information on the identity (i.e. name, address, contact person) of all processors, sub-processors etc. readily available at all times so that they can best fulfil their obligations under Art. 28 GDPR.

Art. 28(1) GDPR provides that controllers have the obligation to engage processors providing 'sufficient guarantees' to implement 'appropriate' measures in such a manner that the processing will meet the requirements of the GDPR and ensure the protection of the rights of individuals. In its Opinion, the EDPB considers that this verification obligation should apply regardless of the risk to the rights and freedoms of individuals. However, the extent of such verification may vary, notably based on the risks associated with the processing.

The Opinion also states that while the initial processor should ensure that it proposes sub-processors with sufficient guarantees, the ultimate decision and responsibility on engaging a specific sub-processor remains with the controller. DPAs should assess whether the controller is able to demonstrate that the verification of the sufficiency of the guarantees has taken place to the controller's satisfaction. The controller may choose to rely on the information received from its processor and build on it if needed. More specifically, for processing presenting a high risk to the rights and freedoms of individuals, the controller should increase its level of verification in terms of checking the information provided. In that regard, the EDPB considers in the Opinion that the controller does not have a duty to systematically ask for the sub-processing contracts to check if data protection obligations have been passed down the processing chain. The controller should assess whether requesting a copy of such contracts or reviewing them is necessary for it to be able to demonstrate compliance with the GDPR.

Transfers outside the EEA

In addition, where transfers of personal data outside of the EEA take place between two (sub-) processors, the data processor as data exporter should prepare the relevant documentation, such as relating to the ground of transfer used, the transfer impact assessment and possible supplementary measures. However, the data controller should assess this documentation and be able to show it to the competent DPA.

Data controller- data processor contracts

The EDPB also addresses, in the Opinion, a question on the wording of controller-processor contracts. In this respect, a basic element is the commitment for the processor to process personal data only on documented instructions from the controller, unless the processor is "required to [process] by Union or Member State law to which the processor is subject" (Art. 28(3)(a) GDPR). In light of the contractual freedom afforded to the parties within the limits of Art. 28(3) GDPR, the EDPB takes the view that including the terms quoted above (either verbatim or in

very similar terms) is highly recommended but not mandatory. As to variants similar to "unless required to do so by law or binding order of a governmental body" the EDPB takes the view that this remains within the contractual freedom of the parties and does not infringe Art. 28(3)(a) GDPR per se. At the same time, the EDPB identifies a number of issues in its Opinion, as such a clause does not exonerate the processor from complying with its obligations under the GDPR. For personal data transferred outside of the EEA, the EDPB considers it unlikely that this variant, in itself, suffice to achieve compliance with Art. 28(3)(a) GDPR in conjunction with Chapter V. Art. 28(3)(a) GDPR does not prevent - in principle - the inclusion in the contract of provisions that address third country law requirements to process transferred personal data. However, a distinction should be made between the third country law(s) which would undermine the level of protection guaranteed by the GDPR and those that would not.

This Opinion contributes to a harmonised interpretation by the DPAs of certain aspects of Art. 28 GDPR, where appropriate, in conjunction with Chapter V GDPR on transfers.

"We would like to express our deep appreciation and gratitude to our European Data Protection Board colleagues, and Secretariat, for guiding the EDPB through the Article 64.2 AI Opinion file, which concluded fittingly at the EDPB's 100th meeting.

Through this intensive process we have collectively secured an important step towards harmonisation at a European level on some of the key issues. This opinion addresses key questions of systemic importance on how responsible AI innovation can be supported by ensuring personal data are protected under the GDPR."

Dr. Des Hogan
Commissioner (Chairperson) for Data Protection, Ireland

Dale Sunderland
Commissioner for Data Protection, Ireland

2.1.2.5 Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models

On 18 December 2024, the EDPB adopted Opinion 28/2024, addressing critical data protection questions surrounding the use of personal data in the development and deployment of Artificial Intelligence (AI) models.

Scope of the Opinion

The Opinion responds to a request from the Irish DPA under Art. 64(2) of the GDPR, with a focus on harmonising regulatory guidance in key areas. It examines the conditions under which an AI model trained on personal data can be considered anonymous. It also evaluates the use of legitimate interest as a legal basis for data processing in the development and deployment of AI models, considering the balance between innovation and individuals' rights.

Furthermore, it assesses the implications of unlawful data processing during an AI model's development and the extent to which such processing affects its subsequent use. While recognising the transformative potential of AI, the Opinion underlines the necessity of aligning technological advancement with the principles of the GDPR, including accountability, transparency, data minimisation, and the right to data protection.

Key considerations

1. Anonymity of AI Models

The Opinion highlights that AI models trained on personal data cannot always be considered anonymous. Claims of anonymity require a case-by-case assessment by DPAs. To establish anonymity, it must be improbable that personal data can be directly extracted or obtained through queries from the model, considering all reasonably likely means of identification. To conduct their assessment, DPAs should review the documentation provided by the controller to demonstrate the anonymity of the model. In that regard, the Opinion provides a non-prescriptive and non-exhaustive list of methods that may be used by controllers in their demonstration of anonymity and thus be considered by DPAs when assessing a controller's claim of anonymity.

2. Legitimate interest as a legal basis

The EDPB emphasises that there is no hierarchy between the legal bases. The Opinion then recalls the three-step test that should be conducted when assessing the use of legitimate interest as a legal basis, i.e. (1) identifying the legitimate interest pursued by the controller or a third party; (2) analysing the necessity of the processing for the

purposes of the legitimate interest(s) pursued (also referred to as "necessity test"); and (3) assessing that the legitimate interest(s) is (are) not overridden by the interests or fundamental rights and freedoms of the data subjects (also referred to as "balancing test"). The Opinion provides practical examples, such as developing AI for fraud detection or cybersecurity, where legitimate interest could apply, provided that strict safeguards are in place.

3. Impact of unlawful processing

Finally, when an AI model was developed with unlawfully processed personal data, this could have an impact on the lawfulness of its deployment, unless the model has been duly anonymised. Opinion 28/2024 reinforces the EDPB's commitment to ensuring that AI innovations respect GDPR principles while enabling responsible technological advancements. The Opinion sets the stage for continued guidance, including forthcoming guidelines on web scraping.

"DPAs' size is not important. Sometimes, even mouses can roar. Dealing with mega-organisations such as those handling adult-content websites, has proved quite a challenge in 2024, but we successfully completed our task. As Deputy Chair of the EDPB I have experienced first-hand the challenges it faces. Yet it is growing stronger. It has proved itself as a major key-player in the international data protection field. In coming years, it will continue improving its image and to provide guidance, where needed."

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

2.2 GENERAL GUIDANCE

The EDPB plays a pivotal role in clarifying and harmonising the application of the GDPR through the issuance of comprehensive guidance.

Since entry into application of the GDPR, the EDPB has established a robust compendium of guidelines that address critical areas of data protection. These efforts have not only reinforced the consistency of enforcement among countries but have also strengthened compliance by offering practical solutions tailored to evolving technological and legal landscapes. The Board's guidelines are developed with a strong emphasis on stakeholder engagement, incorporating feedback gathered through public consultations to ensure they address real-world concerns effectively.

In 2024, the EDPB adopted four guidelines, two of which were finalised following public consultation initiated in 2023. *See Section 4.1 for the complete list of guidelines*.

2.2.1 Guidelines 01/2023 on Article 37 of the Law Enforcement Directive (LED)

Adopted on 19 June 2024, these Guidelines address Art. 37 of the LED concerning cross-border data transfers by law enforcement authorities of EU countries. In particular, they explain the relevant factors to take into account when assessing whether the safeguards put in place for such transfers are "appropriate". The Guidelines build on the previous Recommendations of the EDPB on the adequacy referential under the LED and the EDPB Statement on internal agreements including transfers.

Key recommendations outlined in the Guidelines include:

- **Appropriate safeguards**: they explain the essential requirements for appropriate safeguards to ensure an essentially equivalent level of data protection within the framework of Art. 37;
- **Expectations regarding legally binding instruments**: the EDPB identifies the elements that should, among other aspects, be addressed in such transfer tools (Art. 37(1)(a) LED);
- **Assessment of the transfer circumstances**: the Guidelines provide factors to take into account when competent authorities assess the risk surrounding transfers (Art. 37(1)(b) LED).

By offering this detailed guidance, the EDPB aims to support on the one hand, law enforcement authorities wishing to transfer personal data to third-country authorities or international organisations and, on the other hand, EU countries which negotiate legally binding instruments that serve as tools for such transfers.

2.2.2 Guidelines 02/2023 on the Technical Scope of Art. 5(3) of the ePrivacy Directive

Adopted on 7 October 2024, these Guidelines address the evolving challenges posed by modern online tracking technologies. Art. 5(3) of the ePrivacy Directive regulates the storage and access of information on users' terminal equipment, ensuring such activities are based on user consent or strict necessity.

The Guidelines clarify the scope of this provision, covering technologies such as:

- URL and pixel tracking;
- Local processing;
- Tracking based on IP only;
- Intermittent and mediated Internet of Things (IoT) reporting;
- Unique Identifier.

By dissecting core concepts like "terminal equipment", "information", "gaining access" or "storage" the EDPB ensures that these Guidelines comprehensively address ambiguities, equipping organisations with the tools needed to align their practices with the Directive while safeguarding user privacy.

2.2.3 Guidelines 01/2024 on processing of personal data based on Article 6(1)(f) GDPR

Adopted in October 2024, these Guidelines offer an in-depth exploration of legitimate interest as a legal basis for processing under Art. 6(1)(f) GDPR. The document addresses the three cumulative conditions that must be met:

- **Identification of a legitimate interest**: the interest must be lawful, specific, and present;
- **Necessity of processing**: data controllers must assess whether less intrusive alternatives could achieve the same outcome, ensuring compliance with data minimisation principles;
- **Balancing exercise**: data controllers must weigh their legitimate interest against the fundamental rights and freedoms of individuals, considering factors like transparency, safeguards, and the reasonable expectations of individuals.

Dedicated sections on specific contexts, such as fraud prevention and direct marketing, illustrate the application of these principles, providing stakeholders with insights into how to navigate this area of the GDPR.

2.2.4 Guidelines 02/2024 on Article 48 GDPR

Adopted in December 2024, these Guidelines offer critical clarity on the application of Art. 48 GDPR, which regulates access to personal data by courts and authorities in third countries, and its interaction with Chapter V GDPR.

Key recommendations include:

- **Interaction between Article 48 GDPR and Chapter V GDPR**: where data processed in the EU are transferred or disclosed in response to a request from a third country authority, such disclosure constitutes a transfer within the meaning of Chapter V. As for any transfer subject to the GDPR, there must be a legal basis for the processing in Art. 6 GDPR and a ground for transfer in Chapter V GDPR;
- **Case-by-case assessments**: generally, recognition and enforceability of foreign judgments and decisions is ensured by applicable international agreements which may provide for both a legal basis under Art. 6(1)(c) GDPR or Art. 6(1)(e) GDPR and a ground for transfer under Art. 46(2)(a) GDPR. Where no applicable international agreement exists, or the agreement does not contain a legal basis or appropriate safeguards, the EU data controller or data processor can consider other legal bases and grounds for transfer, including derogations in Art. 49 GDPR.

2.3 STATEMENTS ON LEGISLATIVE DEVELOPMENTS

Legislative developments: context and impact

The year 2024 marked significant advancements in legislative frameworks directly impacting data protection and privacy across the EU. By addressing critical and emerging challenges, the EDPB reinforced its commitment to guiding DPAs and stakeholders through the legislative landscapes.

2.3.1 Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

Recognising the urgency of addressing child sexual abuse online, the EDPB issued Statement 1/2024, which addressed the European Commission's proposed regulation on this critical issue. While acknowledging the importance of combating such crimes, the Board emphasised the need for any measures to comply fully with fundamental rights, particularly the right to privacy and data protection.

The Statement welcomed improvements introduced by the European Parliament, including the exclusion of end-to-end encrypted communications from detection orders. However, it raised concerns over the potential for general and indiscriminate monitoring of private communications, highlighting the high error rates of certain detection technologies. The Board called for proportionality and precision in any proposed measures to ensure compliance with the EU Charter of Fundamental Rights.

This Statement reaffirmed the EDPB's commitment to protecting vulnerable individuals while safeguarding fundamental rights in legislative initiatives.

2.3.2 Statement 2/2024 on the financial data access and payments package

The EDPB's Statement 2/2024 addressed the European Commission's Financial Data Access and Payments Package, comprising the Financial Data Access Regulation (FIDA), the Payment Services Regulation (PSR), and the Payment Services Directive (PSD3). This Statement was adopted in the context of ongoing legislative discussions on this package.

Building upon the practical experience of national DPAs, the Board pointed out to topics where further alignment with the guidelines issued by the EDPB and previous opinions of the EDPS on these proposals should be made.

In particular, the EDPB took note of the European Parliament's reports on the FIDA and PSR proposals, but considered that, with regard to the prevention and detection of fraudulent transactions, additional data protection safeguards should be included in the transaction monitoring mechanism of the PSR proposal. The Board recalled in this regard the need to ensure that the level of interference with the fundamental right to the protection of personal data of persons concerned is necessary and proportionate to the objective of preventing payment fraud.

2.3.3 Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework

In 2024, the EDPB issued Statement 3/2024, which provided comprehensive insights into the role of DPAs within the Artificial Intelligence Act framework. This Statement emphasised the importance of a human-centric approach to AI technologies, ensuring the protection of individuals' fundamental rights, including data protection and privacy, amidst rapid technological advancements.

The Statement recommended that DPAs should be designated as MSAs for high-risk AI systems mentioned in Art. 74(8) of the AI Act. It highlighted the need for enhanced collaboration among DPAs and other regulatory bodies to address cross-sectoral challenges. Furthermore, the EDPB stressed the importance of transparency and accountability in AI deployments, advocating for mechanisms to ensure compliance with the GDPR and the AI Act. In particular, the Statement highlights that a prominent role of the DPAs at national level should be recognised, due to the experience and expertise gathered by them in working out guidelines and best practices and carrying out enforcement actions on AI-related issues with respect to the processing of personal data at both national and international level.

Furthermore, the Statement highlighted the need for enhanced collaboration among DPAs and other regulatory bodies to address cross-sectoral challenges.

"In view of the digital transition, the publication of the AI Act surely constitutes one of the milestones that will shape Europe's digital landscape in the future. It is certain that DPAs will play a crucial role to safeguard rights and freedoms of individuals when personal data are processed in the context of AI."

Dr. Matthias Schmidl
Head of the Austrian Data Protection Authority

2.3.4 Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR

Adopted at the October 2024 plenary, the EDPB's Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR, supported the introduction of procedural rules to harmonise the enforcement of the GDPR across countries. This Statement emphasised the need for clear and consistent rules to

streamline enforcement processes and recommended further addressing specific elements of the regulation to achieve the objectives of streamlining cooperation between authorities and improving the enforcement of the GDPR.

The Board highlighted the importance of ensuring adequate resources for DPAs to implement these procedural rules effectively. It also called for practical measures to support DPAs in managing cross-border cases, thereby promoting consistency and efficiency in enforcement.

By advocating for procedural harmonisation, this Statement represents a significant step towards strengthening the GDPR's framework and ensuring the consistent application of data protection standards throughout the EU.

2.3.5 Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for effective Law enforcement

Adopted in November, the Statement 5/2024 on the recommendations of the High-Level Group (HLG) on access to data for effective law enforcement underlines the importance of safeguarding fundamental rights when law enforcement agencies access personal data. While the EDPB supports the goal of ensuring effective law enforcement, it points out concerns over certain recommendations that could potentially lead to serious intrusions on fundamental rights, particularly privacy and family life.

The EDPB notes positively that the recommendation may contribute to creating a level playing field on data retention. However, it raises concerns that a broad, general obligation for service providers to retain data in electronic form could significantly interfere with individual rights. The Board questions whether this would meet the requirements of necessity and proportionality under the Charter of Fundamental Rights of the EU and the CJEU jurisprudence.

Furthermore, the EDPB stresses that recommendations relating to encryption should not hinder its use or reduce its effectiveness. For example, introducing a client-side process that allows remote access to data before encryption or after decryption would undermine the effectiveness of encryption. Preserving the protection and effectiveness of encryption is critical, not only for respecting private life and confidentiality but also to safeguard freedom of expression and foster economic growth, both of which rely on trustworthy technologies.

2.3.6 Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation - Fostering Cross Regulatory Consistency and Cooperation

During its December 2024 plenary, the EDPB adopted the Statement 6/2024 on the second report of the European Commission regarding the application of the GDPR.

The EDPB welcomes the reports from both the European Commission and the Fundamental Rights Agency, underlining the importance of legal certainty and coherence between digital legislation and the GDPR. It stresses the need for clear and consistent enforcement of the GDPR in the context of the EU's evolving digital landscape. The Board has highlighted its ongoing initiatives, including efforts to clarify the relationship between the GDPR and other critical legislation such as the Artificial Intelligence Act, or those derived from the EU Data Strategy, and the Digital Services Package.

Furthermore, the EDPB confirmed its commitment to enhancing content tailored for non-experts, small and medium-sized enterprises (SMEs), and other relevant groups, to ensure better understanding of data protection principles.

Finally, the Board calls for additional financial and human resources to address the growing complexity of data protection challenges and its expanding responsibilities. These resources are vital for enabling DPAs and the EDPB to continue their work effectively, ensuring high standards of data protection across the EU.

2.4 STAKEHOLDER CONSULTATION

The EDPB upholds its commitment to fostering transparency, inclusivity, and collaboration by actively engaging with stakeholders. These engagements enhance the relevance and practicality of its guidance.

2.4.1 Public Consultation on Guidelines

Public consultations serve as a vital tool for integrating stakeholder perspectives into the EDPB's regulatory framework. By inviting feedback from organisations, advocacy groups, and individuals, the EDPB ensures that its guidelines are aligned with practical realities. Every submission is thoroughly evaluated, and accepted contributions are incorporated into the final documents, reflecting the EDPB's commitment to participatory governance.

In 2024, the Board finalised key consultations that were launched earlier:

- The public consultation on **Guidelines 02/2023** concerning the **Technical Scope of Article 5(3)**

of the ePrivacy Directive concluded in January 2024;

- **Guidelines 01/2024** on the **processing of personal data based on Art. 6(1)(f) GDPR** were completed following a comprehensive consultation;

Additionally, in 2024 the EDPB launched another consultation on **Guidelines 02/2024 on Article 48 GDPR**, which closed in January 2025, further underscoring the EDPB's dedication to continuous stakeholder involvement.

2.4.2 Stakeholder Events

Stakeholder events are pivotal in fostering dialogue and knowledge exchange on emerging issues in data protection. These events not only strengthen the EDPB's understanding of stakeholder concerns but also provide a platform for diverse voices to shape the regulatory landscape.

Two high-profile events in 2024 highlighted the Board's commitment to addressing pressing and complex issues:

- **Consent or Pay models**

  This dedicated event focused on the contentious practice of Consent or Pay models. The event fostered vibrant discussions among a diverse audience, including consumer rights advocates, data protection experts, and industry representatives. Key debates revolved around how these models could comply with the GDPR principles, particularly in ensuring that consent is freely given, and alternatives are genuinely equitable.

- **AI Models and GDPR compliance**

  Another major event addressed the complexities of applying the GDPR principles to AI models, particularly those subject to Art. 64(2) GDPR opinions. The event featured interdisciplinary discussions, drawing insights from academia, legal professionals, NGOs, and industry leaders. Topics ranged from the ethical implications of AI-driven data processing to the practical challenges of ensuring transparency, fairness, and accountability in AI applications.

2.4.3 Survey on Practical Application of Adopted Guidance

Following the 2023 stakeholder survey's results, in 2024 the EDPB implemented most of the recommendations provided improving the accessibility of most guidelines. For instance, in 2023 stakeholders indicated that they considered EDPB's guidance language too technical; moreover they suggested to add visualisations such as videos to provide higher clarity on more technical sections of the guidelines. The EDPB acknowledged that and implemented a series of actions, such as creating less technical factsheets associated to guidelines, including visualisations and flowcharts to help simplify complex information and more.

In addition, in 2023 stakeholders mentioned that adding an executive summary as a standard section of every document would increase the ease of use of the guidelines. In response to that, in 2024 the EDPB included an executive summary to all guidelines to provide a quick overview of the most important points. Additionally, one of the guidelines adopted before public consultation in 2024 - on legitimate interest - featured a factsheet for easier reference. To further enhance clarity, the guidelines on legitimate interest include eight examples. In response to the request made by stakeholders in 2023 for referencing academic work in the guidelines, in 2024 the EDPB made sure to include relevant citations throughout the guidelines. A final input from 2023 was to receive guidance on anonymisation; work on such guidance is currently ongoing showing the EDPB commitment to take into account stakeholders insights and putting them into practice through concrete initiatives.

In 2024, the EDPB conducted its seventh annual stakeholder survey under Art. 71(2) GDPR.

The survey evaluated the effectiveness and clarity of the EDPB's guidelines, opinions, and consultation processes issued throughout the year. It aimed to determine the practical utility of these resources in interpreting the GDPR's provisions and to identify opportunities for enhancing the support provided to organisations and individuals navigating the EU data protection framework.

Survey participants included academics specialising in data protection and privacy rights, legal professionals, business and industry representatives, members of non-governmental organisations and experts from related fields, ensuring a comprehensive range of perspectives was captured.

Among the guidelines most frequently consulted were Guidelines 01/2024 on processing of personal data based on Article 6(1)(f) GDPR and Guidelines 02/2024 on Article 48 GDPR. Stakeholders generally acknowledged these guidelines as helpful resources, providing valuable interpretations of provisions of the GDPR and offering actionable guidance. At the same time, a limited number of stakeholders suggested that certain topics could benefit from more explicit analysis or additional guidance, allowing stakeholders to better understand and navigate challenging scenarios.

Opinions issued by the EDPB also received focused attention from stakeholders, especially Opinion 08/2024 on

Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, along with Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s) and Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models. While many stakeholders found these opinions helpful in interpreting the GDPR, some respondents highlighted areas where they felt some clarification could further enhance their utility. With regard to the opinion on "consent or pay" models, some respondents suggested elucidating how to ensure that consent remains truly "free" when individuals must choose between accepting tracking or paying a fee – namely, how to guarantee that users can decide without undue pressure or economic constraints making tracking the de facto only viable option. They also asked to approach carefully any introduction of new definitions, to avoid unintended impacts on regulatory consistency and clarity. Furthermore, stakeholders encouraged the EDPB to indicate more precisely how any new definitions introduced within the opinion might affect user autonomy, transparency obligations, and reference to existing legal frameworks. According to these respondents, such specificity would bolster both regulatory consistency and the provision of practical, hands-on guidance.

Stakeholders reported primarily accessing EDPB documents via direct search on the EDPB website, complemented by social media channels and informal recommendations. Most indicated regular usage of the guidelines and opinions, generally consulting them monthly or in response to specific issues. To enhance accessibility and ease of use, stakeholders recommended minor improvements, such as consistently including executive summaries. They also advocated for timely official translations, emphasising their importance for applicability across various jurisdictions and stakeholders who operate in multilingual contexts.

Public consultations and stakeholder workshops organised by the EDPB were broadly acknowledged and appreciated. Positive feedback highlighted the well-balanced timeline of consultations, aligning adequately with documents' complexity. At the same time, stakeholders recommended that consultation periods reflect the technical nature and length of documents. Workshops were praised for promoting inclusive dialogue; however, stakeholders suggested improvements to the structure of the sessions, recommending additional opportunities for written input and clearer synthesis of workshop outcomes to maximise effectiveness.

Overall, the 2024 stakeholder survey affirmed widespread appreciation for the structured presentation, practical examples, and clarity provided by EDPB guidance, alongside measured suggestions for enhancement. Stakeholder insights underscore the importance of maintaining clear, consistent, and accessible guidance to support effective implementation and compliance with the GDPR across diverse organisational contexts. The EDPB values the constructive feedback provided and will thoughtfully consider these recommendations in future guidance and consultative practices.

2.5 REPRESENTING THE EDPB WORLDWIDE

In 2024, the EDPB participated in key international fora, fostering strategic collaborations, and addressing critical issues in data protection and privacy. In this way, the EDPB showcased its leadership in shaping robust data protection standards and navigating the challenges posed by rapid digital transformation.

Strategic leadership and Chair's Engagements

Chair Anu Talus spearheaded the EDPB's international initiatives, delivering impactful contributions at 34 high-profile speaking engagements throughout the year. These events highlighted the EDPB's commitment to addressing evolving priorities in data protection and fostering global dialogue. Key highlights included:

- **One-stop-shop roundtable (Paris, February)**: in this commemorative event, Chair Talus delivered a speech stressing the value of cross-border cooperation in addressing emerging data protection challenges;
- **In Cyber Forum (Lille, March)**: during her keynote speech at this forum in France, Chair Talus examined cybersecurity and privacy issues, underscoring the need for robust safeguards and international collaboration;
- **IAPP Global Privacy Summit (Washington, April)**: EDPB Chair gave a speech on "EU DPA Enforcement Priorities and Lessons Learned" offering an in-depth analysis of cross-border enforcement mechanisms and the GDPR's global implications;
- **RSA Conference (San Francisco, May)**: during the panel discussion "AI Governance & Ethics: A Discussion with Leading Voices" the Chair explored the ethical and operational challenges surrounding AI implementation;

- **Privacy Symposium Conference (Venice, June)**: in her opening address, Chair Talus highlighted the significance of international collaboration in addressing privacy challenges across jurisdictions;
- **G7 Data Protection and Privacy Authorities Roundtable (Rome, October)**: Chair Talus actively engaged in strategic dialogues aimed at harmonising global data protection policies and addressing cross-border regulatory challenges;
- **GPA - Global Privacy Assembly (Jersey, November)**: Chair Talus participated to the 46th Global Privacy Assembly, speaking at a panel on "Defining Privacy Harms in a Modern Word" and attending the closed session on "Reporting from other Partner Organizations".

New Deputy Chair appointment

During its June 2024 plenary session, the EDPB elected **Zdravko Vukić**, Director of the Croatian Personal Data Protection Agency, as Deputy Chair. Vukić succeeds Aleid Wolfsen, whose five-year mandate as Deputy Chair concluded, and will work alongside Deputy Chair **Irene Loizidou Nikolaidou** and Chair Anu Talus.

Deputy Chair Vukić expressed his commitment to advancing the EDPB's mission, emphasising the importance of raising GDPR awareness, empowering individuals, and enhancing enforcement cooperation across the EEA. Chair Talus welcomed his appointment, highlighting the opportunity to further bolster the Board's capacity to address its growing tasks and to strengthen collaboration among national DPAs.

Deputy Chair Irene Loizidou Nikolaidou also contributed significantly to the EDPB's international presence, participating in four high profile speaking engagements. These engagements included presentations and panel discussions at various institutes, academic forums, and policy agencies, such as CPDP in Brussels and the Spring Conference in Riga.

Broader EDPB representation

Beyond the contributions given by the EDPB Chair and Deputy Chairs, the EDPB's leadership and staff participated in 43 additional international events, encompassing expert panels, policy workshops, and collaborative discussions. These speaking events covered diverse topics, including:

- Privacy in emerging technologies such as AI and IoT;
- Enhancing regulatory cooperation to ensure seamless cross-border data flows;
- Strengthening compliance mechanisms to uphold data protection standards globally.

Driving Global Impact

The EDPB's international activities in 2024 yielded tangible outcomes, notably:

- Influencing global policy discussions on data protection and privacy through thought leadership and expertise;
- Strengthening partnerships with international stakeholders to promote the harmonisation of data protection standards;
- Sharing best practices and insights to address pressing challenges, including AI governance and digital transformation.

"With the GDPR, Europe has offered the Member States, but also the world, an extraordinary model of innovation governance. The Board can help to promote and disseminate this model, which is based on a sustainable balance between freedom and technology."

Pasquale Stanzione

President of the Italian Data Protection Authority

3. ENFORCEMENT COOPERATION AND ENFORCEMENT BY DPAS

3.1 EDPB ACTIVITIES TO SUPPORT GDPR ENFORCEMENT AND COOPERATION AMONG DPAS

Coordinated Enforcement Framework

The Coordinated Enforcement Framework (CEF) remains a pillar of the EDPB's efforts to strengthen the GDPR compliance across Europe. During its October 2023 Plenary, the EDPB selected the right of access under Art. 15 GDPR as the focus of its third coordinated enforcement action. This decision highlights the importance of the right of access. Such right allows individuals to check if their personal data is handled legally and helps them exercise other rights, like correcting or deleting their data. The EDPB's choice was driven by the significant number of complaints received by DPAs regarding this right and by the adoption in 2023 of Guidelines 01/2022 on the right of access to help data controllers comply with this right.

In 2024, the EDPB officially launched the enforcement action, with 30 participating DPAs actively engaged in the initiative across Europe. The participating DPAs contacted data controllers within their countries to assess compliance with the right of access and whether Guidelines 01/2022 were known and followed in practice. This was implemented through a variety of methods, including the distribution of questionnaires, the commencement of formal investigations where necessary, and the follow-up of ongoing enforcement actions. By utilising a harmonised approach, the CEF allows DPAs to collectively evaluate and address issues related to the implementation of this right.

The first phase of the initiative focused on gathering information and analysing national enforcement practices. A total of 1.185 data controllers were evaluated on key aspects such as response times, clarity, completeness, and overall compliance with access requests under the GDPR. Feedback from DPAs showed a mixed level of compliance across the EU. On the one

hand, some organisations, particularly those with an established internal procedure to handle access requests, demonstrated a strong awareness of their obligations. In that regard, bigger organisations were overall found to be more compliant than small and medium-sized enterprises (SMEs), with less resources. On the other hand, challenges were identified, such as inconsistent and excessive interpretations of the limits to the right of access and barriers that individuals encounter when exercising this right.

The results of this coordinated initiative have been consolidated by the EDPB into a comprehensive report. This report, adopted by the EDPB Plenary in January 2025, provides an aggregated analysis of the findings, offering deeper insights into the level of compliance with the right of access across the EU. Importantly, the report highlights seven areas for improvement and delivers concrete recommendations to enhance consistency, awareness, and enforcement efforts at both national and EU levels. The annex to the report provides the detail of each action at national level.

Support Pool of Experts

The **Support Pool of Experts** (SPE) has continued to play a key role in strengthening the enforcement capacity of DPAs. This initiative, part of the EDPB's Strategy 2024-2027, provides critical technical expertise and tools to address complex cases and emerging data protection challenges. In 2024, nine projects have been launched to enhance the GDPR compliance and enforcement across the EU.

In 2024, the EDPB published the deliverables of seven SPE projects. One of those projects involved creating a case digest on Security of Processing and Data Breach Notification. This initiative provides DPAs with a consolidated repository of decisions, offering valuable insights into recurring issues and thematic trends in enforcement. Another notable project was a new version of the EDPB Website Auditing Tool, which was specifically designed to assist DPAs in evaluating website compliance, including aspects such as cookie management, transparency requirements, and consent mechanisms. The Standardised Messenger Audit project addressed the GDPR compliance challenges in widely used business communication platforms.

The SPE programme also facilitated tailored Data Protection Officer (DPO) training in Croatia. This initiative aimed to equip DPOs with sector-specific expertise to enhance the GDPR compliance, particularly in critical sectors. The AI Risk Assessment project provided tools to address privacy risks in AI systems. For example, it looked at technologies like Optical Character Recognition (OCR), which converts scanned text into readable text, and Named Entity Recognition (NER), which identifies names, organisations, and locations in documents. Complementing this effort, the AI Auditing project developed robust methodologies for auditing AI systems, ensuring their alignment with the GDPR principles such as transparency, fairness, and accountability.

In addition to these initiatives, the EDPB organised a Mobile Apps Bootcamp in September 2024, which built on the success of previous capacity-building events. The bootcamp brought together 50 auditors from 24 countries and the EDPS for a series of expert-led sessions. Presentations were delivered by PEReN (Pôle d'Expertise de la Régulation Numérique) and Dr. Narseo Vallina-Rodriguez, focusing on emerging risks and challenges in mobile applications. Participants also benefited from a practical training session, led by Esther Onfroy, which provided training for compliance assessments of mobile apps. The success of the bootcamp demonstrated the importance of capacity-building and cross-border collaboration in addressing new data protection challenges.

Memorandum of Cooperation with PEReN

In April 2024, the EDPB signed a Memorandum of Cooperation with PEReN, an interdepartmental office operating under the joint authority of the French Ministers of Economy, Culture, and Digital Technology. This agreement represents a significant milestone in enhancing technical collaboration to address emerging data protection challenges across Europe.

As a recognised centre of expertise in data science and algorithmic transparency, PEReN provides technical support to regulators and administrations. The Memorandum formalises a partnership aimed at advancing expertise in critical areas such as mobile application auditing, innovative data science methodologies, and ensuring transparency in algorithmic systems. A particular focus of the cooperation lies in sharing knowledge on tools to support trustworthy artificial intelligence, prioritising the monitoring and auditing of AI systems for GDPR compliance.

This partnership reinforces the EDPB's strategic commitment to leveraging technical expertise to navigate the increasingly complex data protection landscape. By fostering collaboration with specialised institutions like PEReN, the EDPB ensures that European data protection standards remain robust and adaptive in the face of evolving technological advancements.

Chat GPT taskforce

In 2024, the rapid advancements in artificial intelligence (AI) and the growing influence of large language models prompted the EDPB to take decisive action within its ChatGPT Taskforce.

The genesis of this taskforce was rooted in an absence of a unified enforcement mechanism under the one-stop-shop framework, as OpenAI had no EU establishment

prior to February 2024. The taskforce emerged as a collaborative effort to bridge gaps, ensure consistent application of the GDPR, and tackle the unique risks associated with ChatGPT's processing activities.

From its inception, the taskforce adopted an innovative and proactive approach. Multiple sessions brought together representatives from participating DPAs, fostering a dynamic exchange of information and strategies. A standardised questionnaire was developed as a foundational tool, allowing DPAs to investigate ChatGPT's practices uniformly across borders. This cohesive methodology reinforced the EDPB's commitment to ensuring data protection principles were upheld, even in the face of unprecedented technological complexities.

Key areas of investigation included data accuracy, transparency, fairness, and compliance with individual rights. The taskforce uncovered significant challenges, such as risks associated with web scraping, the processing of personal data in model training, and the generation of outputs that may not align with the GDPR principles. Preliminary findings highlighted the necessity of embedding "data protection by design and by default" into AI systems to mitigate these risks and reinforce accountability for data controllers managing personal data on an unprecedented scale.

The taskforce's work also emphasised the importance of international cooperation and expertise. By engaging with stakeholders and experts in AI, the EDPB demonstrated its capacity to adapt to evolving technological landscapes and to ensure robust enforcement mechanisms are in place for future AI-related developments.

Through the ChatGPT Taskforce, the EDPB not only reaffirmed its role as a guardian of individuals' digital rights but also set a precedent for addressing emerging challenges in the era of artificial intelligence. This initiative serves as a benchmark for future collaborations, reinforcing the GDPR's relevance in navigating the complexities of the digital age.

Secondment Programme

The EDPB Secondment Programme has evolved into a cornerstone of cross-border cooperation, fostering a spirit of collaboration and shared expertise between DPAs across Europe. Initially launched as a pilot project in 2019, the programme's success and growing popularity among countries led to its formalisation in 2024, marking a significant milestone in the EDPB's efforts to strengthen the GDPR enforcement.

In 2024, the programme facilitated 61 secondments across 27 authorities, providing participants with invaluable opportunities to deepen their expertise and enhance their operational capabilities.[6] Following the matching of secondees with hosting authorities, a two-day training session has been held in Brussels in September 2024, organised by the EDPB Secretariat. During this training, secondees were able to learn more about the EDPB's activities, the EDPB Secretariat, the EDPS, the EU-wide enforcement and cooperation initiatives and had the opportunity to visit the EU institutions.

These secondments do not only enable participants to exchange practical knowledge and insights but also allow them to observe different enforcement approaches and best practices in diverse regulatory environments. For many, the experience extends beyond technical learning, fostering professional networks and long-lasting relationships that underpin cooperation among DPAs.

The tangible benefits of the programme resonate at both institutional and individual levels. Host authorities gain fresh perspectives and additional resources to address complex data protection challenges, while sending authorities benefit from the enhanced skills and knowledge their secondees bring back. This reciprocal value strengthens the collective capacity of the EDPB network, ensuring a harmonised and effective implementation of the GDPR requirements.

3.2 COOPERATION UNDER THE GDPR

The GDPR establishes a robust framework for collaboration among national DPAs, ensuring a harmonised approach to data protection enforcement across the EU. This cooperation is operationalised through mechanisms such as mutual assistance, joint operations, and the one-stop-shop mechanism, which collectively enhance the consistency and effectiveness of enforcement efforts.

In 2024, the EDPB's cooperative initiatives achieved remarkable milestones. The case register documented 350 cross-border cases, underscoring the high degree of coordination among DPAs in tackling complex, cross-jurisdictional data protection issues. Simultaneously, 982 procedures were initiated under the one-stop-shop mechanism, culminating in 485 final decisions. These figures reflect the operational efficiency and effectiveness of the GDPR's cooperation mechanisms

[6] The selection process took place before the summer 2024 while the secondments have taken place or will take place until end of 2025.

in delivering harmonised enforcement and upholding individuals' rights across the EU.

The outcomes of these initiatives demonstrate the critical importance of close collaboration between DPAs. By leveraging mutual assistance and conducting joint operations, the EDPB ensures that organisations remain accountable for their GDPR obligations, irrespective of their geographical location within the EU.

This collaborative approach not only fortifies trust in the GDPR framework but also demonstrates the EU's commitment to safeguarding the fundamental rights of individuals in an increasingly interconnected digital environment.

Please note that:

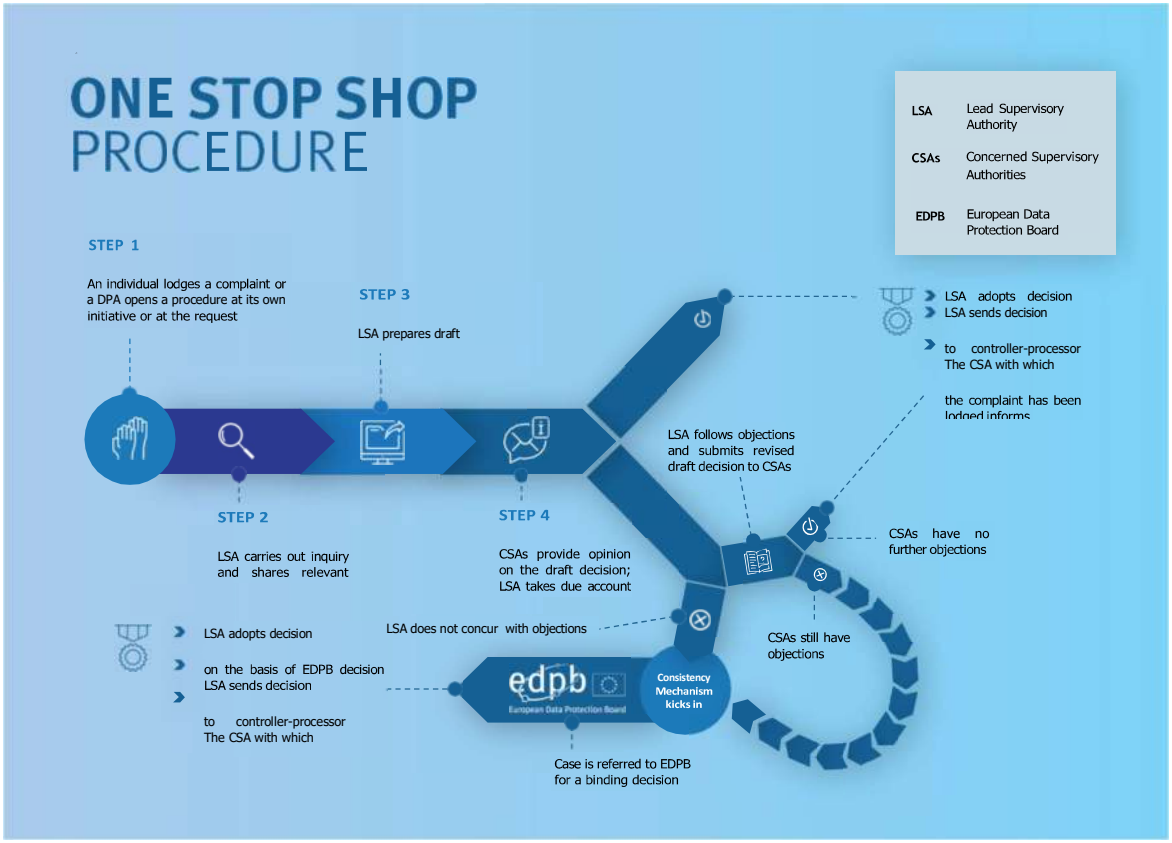
- References to case register entries in these statistics do not have a 1-to-1 correlation to the number of cross-border complaints handled per country as multiple complaints may be bundled in one case register entry, which therefore can relate to multiple cross-border cases;
- Depending on the Member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

3.3 BINDING DECISIONS

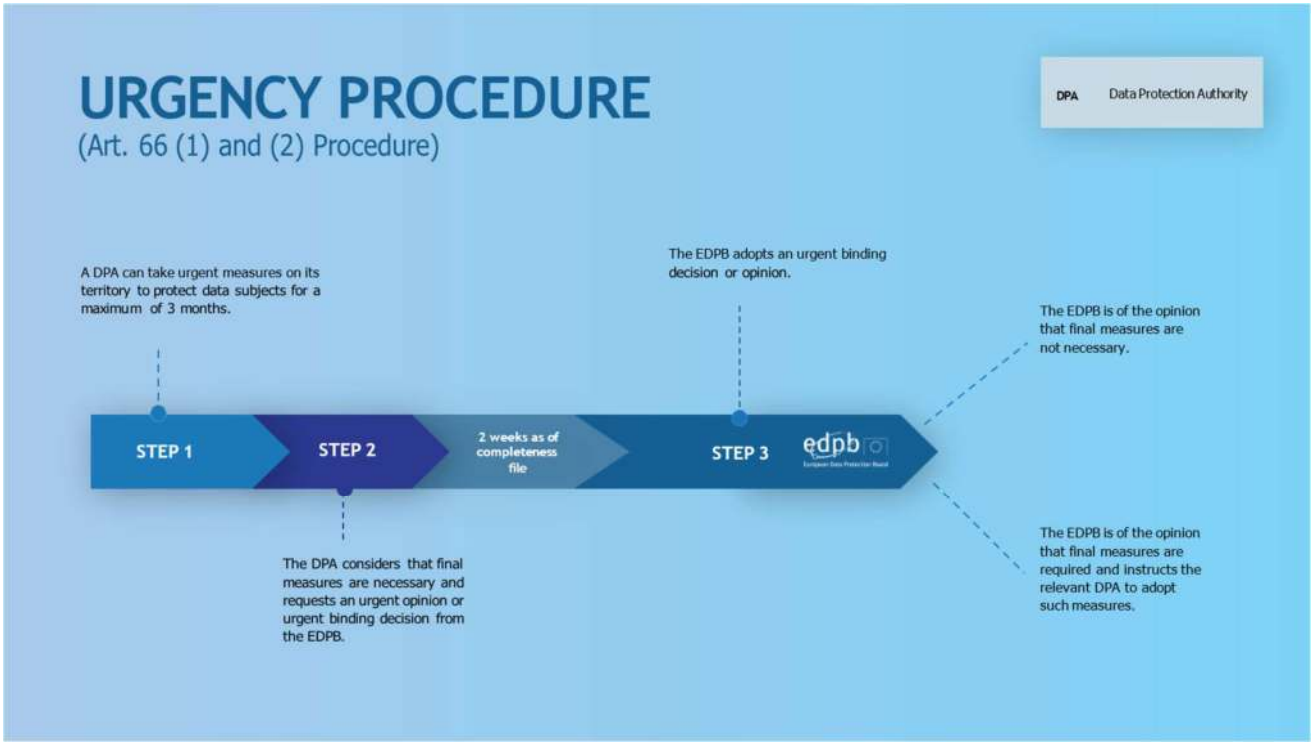
The EDPB plays a critical role in resolving disputes between DPAs and ensuring the consistent application of the GDPR through its binding decision-making powers under Art. 65 GDPR and Art. 66 GDPR. These powers help resolve disagreements in cross-border cases under the one-stop-shop mechanism. They also allow urgent action when needed.

In 2024, no binding decisions were adopted by the EDPB. This shows progress in building consensus and cooperation among DPAs. The consistent dialogue facilitated by the EDPB has allowed DPAs to resolve cases more efficiently at the national level, contributing to a more harmonised enforcement landscape across the EU.

Looking ahead, the EDPB remains prepared to exercise its binding decision-making powers as necessary to uphold the uniform application of the GDPR and address any unresolved disputes that may arise in the future.



In previous years, binding decisions have provided clarity on complex cases involving major organisations, addressing high-profile issues that impact individuals across the EU. They have also set significant precedents for GDPR enforcement, often leading to notable financial penalties and reinforcing accountability among data controllers and data processors. The urgency procedure in Art. 66 GDPR allows rapid action to maintain compliance in critical situations.



3.4 CASE DIGEST

For the third time,[7] 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 Hanne Marie Motzfeldt[8] drafted a case digest based on the decisions adopted under the one-stop-shop mechanism regarding the right of access that are available in the EDPB register.[9] More specifically, these decisions relate to Art. 15 GDPR ('Right of access by the data subject') and also briefly touch upon Art.12 GDPR ('Transparent information, communication and modalities for the exercise of the rights of the data subject'). The right of access of data subjects is enshrined in Art. 8 of the EU Charter of Fundamental Rights, and a large volume of decisions is available in the EDPB register on this matter.

More specifically, the SPE expert identified 185 decisions in the EDPB register, which were adopted between January 2019 and April 2024. As the SPE expert found similarities between some of these decisions, a total of 52 decisions have been selected to be included in the one-stop-shop case digest.

According to the SPE expert, the enforcement of Art.12 GDPR and Art.15 GDPR significantly supports data subjects in effectively invoking their right of access across the EEA. Almost all of the one-stop-shop decisions reviewed originate from complaints and involve almost exclusively data controllers in the private sector. Complaints often arose in a commercial context, i.e. between the data controllers and its users or customers, and revolved mainly around social media and online environments.

The one-stop-shop case digest summarises how DPAs interpret the different components of the right of access, in different contexts, namely: (1) the confirmation as to whether personal data is processed or not, (2) access to

[7] Case digest on the right to object and the right to erasure, Alessandro Mantelero, 9 December 2022; Case digest on security of processing and data breach notification, Professor Eleni Kosta, 27 November 2023. All the previous case digests are available at https://www.edpb.europa.eu/about-edpb/publications/one-stop-shop-case-digests_en.

[8] Professor in Administrative Law and Digitalisation at the University of Copenhagen, Ph.D. in Law.

[9] EDPB's public register with the one-stop-shop final decisions is available at https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions; 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.

and copy of such personal data, and (3) access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers. In addition, the digest also analyses previous cases where exceptions and limitations to the right of access were raised by data controllers. Overall, the case digest provides useful examples on the exercise of the right of access in various contexts, for instance in the event of fake profiles or accounts which impersonate data subjects.

DPAs do not automatically impose corrective measures in one-stop-shop decisions on the right of access. On the contrary, they often dismiss or settle the case if the matter has been resolved during the course of the proceedings.

The case digest also refers to the available guidance at EU level, and in particular, EDPB Guidelines 01/2022 on data subject rights – Right of access, adopted on 28 March 2023. Relevant cases before the Court of Justice of the EU (CJEU) are mentioned. In that regard, the reviewed one-stop-shop decisions often rely on the (growing) case law of the CJEU in the field of the right of access and have recently started to refer to the EDPB Guidelines on the right of access.

3.5 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 data processor where its intended processing operations are likely to infringe the GDPR;
- Issuing reprimands to a data controller or data processor where processing operations have infringed the GDPR;
- Ordering a data controller or data 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 2024, DPAs issued a number of fines, as indicated in the table below.

DPA	Num-ber of fines	Total Fines amount
Austria	63	€1 682 88
Belgium	8	€708 371
Bulgaria	25	€159 885
Croatia	38	€552 200
Cyprus	22	€133 900
Czech Republic	18	€13 882
Denmark	4	€298 657
Estonia	9	€164 100
Finland	3	€4 206 000
France	87	€55 212 400
Germany (all Länder grouped together)	416	€13 802 044
Greece	22	€4 301 249
Hungary	26	€853 788
Iceland	1	€9 961
Ireland	7	€652 029 500

DPA	Number of fines	Total Fines amount
Italy	140	€145 332 449
Latvia	14	€6 150
Liechtenstein	3	€22 911
Lithuania	13	€2 423 971
Luxembourg	1	€2 300
Malta	3	€18 000
Netherlands	16	€ 328 030 000
Norway	4	€ 63 000
Poland	25	€3 053 976
Portugal	23	€138 375
Romania	83	€371 116
Slovakia	38	€85 200
Slovenia	5	€51 000
Spain	281	€35 592 200
Sweden	6	€5 280 000
		€1 254 684 666

3.6 SELECTION OF NATIONAL CASES

This section of the Annual Report 2024 presents a non-exhaustive selection of national enforcement actions undertaken by DPAs across various EEA countries.[10] The cases highlighted here illustrate the diverse regulatory responses to GDPR infringements, ranging from investigations and compliance orders to significant sanctions and fines. Many of these cases highlight recurring challenges, such as:

- Insufficient technical and organisational measures to secure personal data;
- Processing conducted without a proper legal basis, including instances where consent was not obtained;
- Unlawful processing of special categories of personal data (e.g. health data);
- Failure by data controllers to provide clear information on their processing activities and to uphold individual rights, such as the right to erasure and the right of access;
- Lack of notification of data breaches or inadequate assessment of the associated risks.

Several of the cases presented were resolved through the one stop shop cooperation mechanism, reflecting the coordinated effort at both national and European levels to ensure consistent application of the GDPR. While this selection does not examine all enforcement actions, it demonstrates the strong commitment of national DPAs to safeguard individuals' digital rights.

3.6.1 AUSTRIA

In 2024, the AT DPA performed 647 investigations, received 3.491 complaints and adopted 63 sanctions corresponding to €1.682.880 of fines. These relate among other, to unlawful processing of (sensitive) personal data due to an infringement of data protection principles (Art.5, Art. 6 and Art. 9 GDPR- most frequent infringement), infringement of data subjects' rights (Art.15 to Art. 22 GDPR - second most frequent infringement) and infringement of the obligation to cooperate with the AT DPA (Art. 31 GDPR - third most frequent infringement).

Two cases are presented in this section.

Case 1: The AT DPA imposed a fine of €1.5 million in August 2024 for the unlawful operation of a video surveillance system comprising several external and internal cameras (violation of Art. 5 GDPR and Art. 6 GDPR). The authority took into account a recent CJEU ruling, which established that the concept of "undertaking" under Art.101 and Art. 102 TFEU must be applied when calculating GDPR fines to ensure compliance with the requirements according to Art. 83(1) GDPR — effectiveness, deterrence, and proportionality (CJEU 05.12.2023, C-807/21, Deutsche Wohnen, ECLI:EU:C:2023:950). The fine was imposed on an organisation that was part of an undertaking, within the meaning of Art. 101 and Art. 102 TFEU, ensuring that the actual economic capacity of the entity was considered in determining the fine.

Case 2: In 2024, it was reported in the media that two federal states were planning an anonymised “abortion register”. The AT DPA then initiated two ex officio investigations. One federal state stated that no abortion register was planned, which is why this ex officio investigation was discontinued. In the case of the other federal state, the investigations revealed that the entries in the planned abortion register were to be anonymous and aimed to identify supply bottlenecks and the risks of abortions and teenage pregnancies. However, the AT DPA had doubts as to whether anonymisation was sufficient in all cases. Likewise, the purposes of an abortion register (such as supply bottlenecks) did not appear to be compatible with the tasks of the (sole) data controller (registering medical practices or clinics). The DPA issued a warning pursuant to Art. 58(2)(a) GDPR for lack of a legal basis.

3.6.2 BELGIUM

In 2024, the Belgian DPA performed 130 investigations, received 469 complaints, issued 24 compliance orders and adopted eight financial sanctions corresponding to €708.371,00 of fines. These relate among other, to a data breach in a hospital, a data broker and the processing of biometric data.

Three cases are presented in this section.

Case 1: The Cumuleo.be case

The Belgian DPA received a cross-border complaint from the CNIL (French DPA) regarding the publication of the complainant's salary on the Belgian website Cumuleo.be. The Belgian DPA determined that the website had rightfully rejected the complainant's erasure request, as the publication of this data is necessary for exercising the right to freedom of expression and information, pursuant to Art. 17(3) GDPR. The Belgian DPA considered, in this particular instance, that the public interest in having access to this information outweighed the complainant's right to have their personal data erased from the website. Pursuant to Art. 60(3) and 60(8) GDPR, the Belgian DPA,

[10] This selection of cases and figures includes those that were sent to the EDPB by the DPAs following a request to submit national enforcement news. Figures were collected between December 2024 and January 2025. The EDPB is not responsible for the accuracy of the information collected. Further cases can be found on https://edpb.europa.eu/news/news en.

acting as the Lead Supervisory Authority (LSA) in this case, submitted a draft decision proposing to dismiss the complaint to the CNIL (with which the complaint was lodged). The CNIL raised no objections and issued its final decision on 7 August 2024.

Case 2: A cookie banner case

In September 2024, The Belgian DPA took action against Mediahuis for the unlawful use of cookie banners. The Belgian DPA had received complaints from a Dutch citizen, represented by NOYB, for four Mediahuis press websites regarding their cookie banners. The Belgian DPA reiterated that the use of deceptive design patterns is unlawful and, consequently, that the "agree and exit" button ("accept all") should not be more prominent than another option. It recommended that both "accept all" and "reject all" options be displayed in an equivalent manner and at the same level.

The Belgian DPA ordered Mediahuis to adapt its cookie banners without using misleading button colours. In case of non-compliance after 45 days following the decision, Mediahuis must pay a €25.000 penalty per day. An appeal on the merits against this decision is still ongoing.

Case 3: A data broker case

In January 2024, The Belgian DPA imposed a total of €174.640 in administrative fines as well as corrective measures on Black Tiger Belgium, an organisation specialising in big data and data management, for various breaches of the GDPR. This penalty covers, among other things, the unfair processing of data without having proactively, individually and transparently informed the people whose data was being processed. The Belgian DPA has also noted violations linked to the exercise of data protection rights and the register of processing activities. A summary is available here.

Link to annual report of Belgian DPA: https://www.autoriteprotectiondonnees.be/citoyen/l-autorite/rapport-annuel

3.6.3 BULGARIA

In 2024, the Bulgarian DPA performed 968 investigations, received 824 complaints, issued 38 compliance orders and adopted 25 sanctions corresponding to €159.885 of fines.

3.6.4 CROATIA

In 2024, the Croatian DPA performed 623 investigations, received 1.280 complaints, issued 153 compliance orders and adopted 191 sanctions corresponding to 38 of fines. These relate among other, to the data breach concerning owners of registered vehicles in Croatia, processing of personal data of owners of business entities, processing of personal data via cookies and video surveillance, appointment of DPOs and in appropriate technical and organisational measures to protect sensitive data, including health data.

Three cases are presented in this section.

Case 1: The Croatian DPA received several complaints from data subjects stating that they had requested copies of their health data. However, the hospital failed to provide the copies, stating that the requested medical documentation had been irretrievably lost. As the hospital had not created backups of such personal data, access to the data subjects' personal data was entirely lost, resulting in a breach of Art. 32(1)(b) GDPR. In addition, the Agency determined that the hospital violated the following provisions of the GDPR: Art. 33(1), Art. 28(3), Art. 6(1), Art. 5(1)(e), Art. 12(1), Art. 13(1)(c), Art. 13(2)(a)(b), and Art. 38(1). As a result of these infringements, the Croatian DPA imposed an administrative fine of €190.000.

Case 2: In the investigation conducted by the Croatian DPA against an organisation whose primary business activity involves parking fee collection and parking supervision, it was determined that the data controller was processing personal data of at least 27.122 individuals for unlawful purposes and without establishing a lawful basis. This personal data was obtained through the web service of the Ministry of the Interior of the Republic of Croatia. The processing was carried out without a legal basis, in violation of Art. 5(1)(b) and contrary to Art. 6(1) GDPR. Additionally, the data controller failed to implement adequate organisational and technical measures, violating Art. 32(1)(b) and Art. 32(4) GDPR. As a result of these infringements, the data controller was imposed a fine of €80.000.

Case 3: In the investigation conducted by the Croatian DPA against a data controller whose primary business activity involves providing basic and financial data on business entities through a platform available on its website, it was determined that the data controller was processing personal data in violation of Art. 6(1)(f), in conjunction with Art. 5(1)(a) and (e) GDPR. In addition, violations of Art. 12, Art. 13, Art. 14, Art. 30, and Art. 38(3) and (6) GDPR have been identified. As a result, the rights of 170,782 individuals were infringed. For these violations of the GDPR, an administrative fine of €40.000 has been imposed.

Link to annual report of the Croatian DPA: https://azop.hr/godisnja-izvjesca-o-radu/.

3.6.5 CYPRUS

In 2024, the CY DPA performed 44 investigations, received 513 complaints, out of which 115 concerned spam, issued 23 compliance orders and adopted 22 sanctions corresponding to a total of €133.900,00 of fines (€9.000.00 for

five cases concerning spam). Out of the remaining 17 sanctions, 10 cases related to breach of Art. 5(1)(f) GDPR, 24(1) GDPR and 32(1) GDPR, four cases concerned Art. 12 GDPR, one case related to Art. 28(3) GDPR and Art. 35 GDPR, one case concerned Art. 5(1)(c) GDPR, and one case related to breach of Art. 15 GDPR. Two cases are presented in this section:

Case 1: **Aylo Freesites Ltd**

The CY DPA performed an ex officio audit of Aylo Freesites Ltd, which owns and operates a number of worldwide known adult content websites. The audit investigated the organisation's compliance with the GDPR, focusing on issues such as cookie consent, biometric data processing via a third-party, DPIAs, and data processing agreements. The Commissioner identified several violations of the GDPR, leading to a preliminary decision and subsequent fines totalling €48.000 and an additional €10.400 for the non-compliant use of cookies. Aylo Freesites Ltd responded to the findings and implemented corrective measures, resulting in a final decision that while imposing fines, acknowledged their efforts towards compliance.

In summary, Aylo Freesites Ltd. demonstrated a lack of adherence to several key data protection principles including accountability, transparency, lawfulness, fairness, data minimisation, storage limitation, data security, and the necessity of a legal basis for processing.

Case 2: State Health Services Organisation (SHSO)

The CY DPA investigated 13 data breach notifications submitted by the SHSO. 10 of these concerned loss of patients' medical files and three concerned the loss of patients' registration forms at Accident and Emergency Units. Each notification concerned a separate patient.

Even though the conditions and circumstances of each data breach were different, the investigations revealed that SHSO did not have in place appropriate technical and organisational measures (Art. 24(1) GDPR and Art. 32(1) GDPR). Its written medical file management procedure was not adequate to prevent loss of medical files and registration forms. It was concluded that patients' personal data were not processed in a manner that ensured appropriate security (Art. 5(1)(f) GDPR).

A total fine of €46.500 was imposed onto the SHSO for the reported losses: €5.000 for each of the nine medical files lost and €500 for each lost registration form. For one medical file, the Commissioner issued a reprimand since SHSO was not in a position to confirm if a file for the specific patient had been created. Reprimands were issued in two other cases, due to SHSO's delay in submitting a data breach notification to the CY DPA. In seven cases, the Commissioner ordered SHSO to communicate the breaches to the affected data subjects.

3.6.6 CZECH REPUBLIC

A fine of CZK 351 million (approximately €13.9 million) was imposed by the Czech DPA on a data controller (software organisation) for infringing Art. 6 GDPR and Art. 13 (1) GDPR. This case was dealt with through the one-stop-shop mechanism with the Czech DPA as the Lead Supervisory Authority (LSA) and all other DPAs involved as Concerned Supervisory Authority (CSA).

The Czech DPA found that the data controller collected and transferred personal data of the users of its antivirus software and its browser extensions to its sister organisation without due legal title for such processing at least during a period between April and July 2019. The transferred data related to roughly 100 million users and comprised especially pseudonymised internet browsing history of the users, tied to a unique identifier. Further, the LSA found that the data controller misinformed its users (individuals) about the said data transfers, as it claimed that the transferred data were anonymised and used solely for statistical trend analytics. The LSA concluded that internet browsing history, even if not complete, may constitute personal data, since re-identification of at least some of the data subjects could occur. The data controller's infringement is even more serious considering that it is one of the foremost experts on cybersecurity that offers tools for data and privacy protection to the public.

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

3.6.7 DENMARK

In most EEA jurisdictions, DPAs have the power to issue administrative fines. In Denmark, however, this is not the case. Instead, data protection law infringements may – taking into account the seriousness of the offence – be reported by the Danish DPA 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 2024, the Danish DPA performed 518 investigations, received 1.777 complaints, and proposed (by own volition) four sanctions of at least €2.98 million in fines. Two key cases are worth mentioning in this section.

Case 1: In the first case, the Danish DPA has reported a municipality to the police for violating Art. 32 GDPR. The municipality had not encrypted up to 300 computers on which personal data was at risk of being processed. Three of the computers were stolen and they contained personal data of confidential and sensitive nature about children. It was noted in the case, that the Danish DPA believes that encryption is a basic security measure that is relatively easy and not very expensive to implement. The police are now conducting an investigation to determine whether charges should be filed, and if that is the case the Court will then decide the amount of the fine. The Danish DPA has recommended a fine of €26.000.

Case 2: In the second case, the Danish DPA decided to initiate a general investigation regarding private sector data controllers' supervision of their data processors. The investigation led to a private hospital being reported to the police for failing to supervise their three data processors to the required extent and thereby violating the principle of responsibility according to Art.5(2) GDPR. The assessment was that the private hospital was not able to ensure and demonstrate that personal data was processed in accordance with the general principles of the Art. 5(1) GDPR. The Danish DPA has recommended a fine of €200.000.

3.6.8 ESTONIA

In 2024, the Estonian Data Protection Inspectorate (EDPI) received in total 733 complaints and 184 data breach notifications affecting over 910.000 individuals. The EDPI issued 116 compliance orders, conducted 73 own initiative inspections and adopted nine sanctions corresponding to €164.100 in fines and penalty payments. In this section three cases are presented:

Case 1: The EDPI issued a fine of €85.000 to Asper Biogene OÜ. The offence consists of two misdemeanours. The first offence consists of inadequate security measures for processing personal data. For failing to ensure the security of processing of personal data in accordance with the requirements of the GDPR, the EDPI imposed a fine of €80.000. The second offence is the breach of the duty to avoid conflicts of interest in the appointment of a data protection officer or data protection specialist (DPO) and the duty to appoint a competent DPO. For that the EDPI issued a fine of €5.000.

Case 2: In 2024, the Estonian DPA also dealt with a case concerning the Viljandi Hospital where 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. The Estonian DPA issued a fine of €40.000 to the Viljandi Hospital. The Viljandi Hospital appealed against the fine decision and was successful at first instance, which the EDPI is appealing.

Case 3: Lastly the EDPI has an ongoing supervision for a data leakage that included approximately 700.000 files with personal and health data. It took place in the beginning of 2024 and was one of the biggest leakages of all time for Estonia with files consisting sensitive data.

3.6.9 FINLAND

In 2024, the Finnish DPA conducted 9 audits, received 1.932 complaints, issued 9 compliance orders and adopted 3 sanctions corresponding to €4.206.000 in fines. The fines relate to defining a storage period for customer data, lawfulness of processing, and neglecting data security. Three cases are presented in this section.

Case 1: An administrative fine of €2.4 million was imposed on Posti for unlawful processing of personal data (Art. 6(1) GDPR). The organisation had automatically created an electronic mailbox for customers without a separate request and was processing personal data on the basis of a contract. The contract included a wider set of services. The Finnish DPA considered that the service requested by the customer could have been provided without the automatic creation of an electronic mailbox. The organisation did also not inform its customers clearly about the activation of the mailbox, and there were technical settings in the service that did not meet data protection requirements. The organisation was reprimanded for the shortcomings and was ordered to correct its unlawful practices (Art 5(1)(a) GDPR, Art. 12(1) GDPR, Art. 13(1)(c) GDPR and Art. 25(1) GDPR). Two cases are presented in this section.

Case 2: The Finnish DPA imposed an administrative fine of €856.000 on the online retailer Verkkokauppa.com Oyj because it had not specified the storage period of customer account data (Art. 5(1)(e) GDPR). The organisation's practice of requiring the creation of a customer account to make online purchases also violated data protection law. The organisation was ordered to specify an appropriate storage period for customer account data and rectify its practice of mandatory registration (Art. 5(1)(e) GDPR and Art. 25(2) GDPR). The organisation was also reprimanded.

Case 3: The loan comparison provider Sambla Group was issued an administrative fine of €950.000 for data security neglect (Art. 5(1)(f) GDPR). Due to poor data security in the loan comparison services, the contents of customers' loan applications had been accessible to third parties through personal links. The organisation was ordered to cease processing the personal data its electronic services when the seriousness of the issues became apparent in March 2024. In December 2024, a fine was imposed on the organisation, and it was reprimanded for its data protection shortcomings (Art. 5(1)(f) GDPR, Art. 25 GDPR and Art. 32 GDPR). It was also ordered to notify its customers of the data breach.

3.6.10 FRANCE

In 2024, the French DPA performed 321 investigations, received a total of 17.193 complaints and closed 15.266 complaints, issued 180 compliance orders, 64 reprimands and a total of 87 sanctions corresponding to €55.2 million of fines. Under the GDPR only, it adopted 60 sanctions corresponding to €3.7 million of fines. These relate among other, to rights of individuals, legal basis, retention periods or security of personal data. This section emphasizes two significant cases.

Case 1: On April 4th 2024, the CNIL fined HUBSIDE.STORE €525.000 for having used data supplied by data brokers

for commercial prospecting purposes, without ensuring that the individuals concerned had given their valid consent (LSA: France; CSA: Belgium, Italy, Portugal, Spain).

Case 2: On 5 December 2024, the CNIL imposed a fine of €240.000 on KASPR since it collected contact details of users on LinkedIn, even if they previously masked them (LSA: France; CSA: all DPAs)

3.6.11 GERMANY

There are both national (federal) and regional DPAs in Germany. Three cases are highlighted in this section.

Case 1: The Bavarian DPA has concluded its investigation into the processing of biometric data by the organisation "Worldcoin" with an initial order. "Worldcoin" offers a digital service for human verification and a cryptocurrency, which, among other things, is based on blockchain technology. At the center of its concept is the so-called World ID, which is intended to provide proof that a stakeholder is a unique human being. Despite the improvements already initiated, further adjustments are necessary. The organisation has been ordered, among other things, to implement a deletion procedure in compliance with the GDPR regulations. In addition, "Worldcoin" is required to obtain explicit consent for certain processing steps in the future. Furthermore, the DPA has mandated the deletion of certain datasets that were previously collected without sufficient legal basis.

Case 2: The DPA of Lower Saxony responded to numerous complaints and conducted spot checks on 17 branches of 10 fitness companies and investigated additional gyms that stood out for specific reasons. The review focused on video surveillance systems, information obligations, and other formal requirements. In some cases, the DPA identified serious data protection violations and imposed fines. Three companies unlawfully monitored training areas, seating areas for customers, and employee spaces within their gyms. Additionally, two companies improperly filmed areas outside their premises. In another case, the DPA imposed a fine due to various technical-organisational deficiencies. For instance, unencrypted data backups were stored on a USB stick attached to the managing director's keychain and in the private residence of an employee.

Case 3: The Hamburg DPA audited companies with a strong market presence in the field of credit collection services. The companies were sent detailed questionnaires and were asked to provide documents such as the directory of processing activities, lists of security measures, and sample letters used. Following the written examination some companies were checked at their business premises. In the case of one organisation a six-digit number of data records with personal data had been stored without a legal basis, some of them five years after the legal retention period had expired. The Hamburg DPA penalised the violation with a fine of €900.000.

3.6.12 GREECE

In 2024, the Greek DPA conducted four on-site inspections, received 1.820 complaints, issued 18 orders and imposed sanctions in 22 GDPR cases amounting to €4.3 million in fines, relating to, inter alia, security of processing, data breach, lawfulness, fairness and transparency, integrity and confidentiality, DPIAs, records of processing activities, data protection by design, responsibility of the data controller and cooperation with the DPA.

In the following section three cases are presented:

Case 1: In April 2024, the Greek DPA imposed a €175.000 fine and issued a compliance order to the Ministry of Migration and Asylum for violations related to the "Centaur" and "Hyperion" systems used in the reception and accommodation facilities of non-EU country nationals on the Aegean islands. The Greek DPA found a lack of cooperation on the part of the Ministry, as data controller, and further considered that the required DPIAs carried out by the Ministry were substantially incomplete and limited in scope, and that serious shortcomings remained as regards the Ministry's compliance with certain provisions of the GDPR in relation to the implementation of the systems in question.

Case 2: In May 2024, the Greek DPA imposed a fine to the Ministry of Interior (€400.000) after a major data leak involving expatriate voters' personal information. The investigation, which began after numerous complaints about unsolicited political communication via e-mail on an initiative related to the European elections by one of the data controllers, revealed unauthorised transfer of data, including email addresses and telephone numbers, outside the Ministry, leading to multiple infringements of the GDPR. In addition to the fine, the Ministry has been instructed to implement corrective measures to ensure compliance with the GDPR regulations within a specified timeframe. A second data controller involved in the case was also fined (€40.000) for the GDPR violations and ordered to delete unlawfully processed data.

Case 3: In September 2024, the Greek DPA imposed a total fine of €150.000 to the Ministry of Citizen Protection for issues arising from the introduction of the new type of identity cards for Greek citizens. In particular, the Greek DPA identified shortcomings on the provision of information to the data subjects, while it further concluded that the required DPIAs was carried out belatedly and had deficiencies. The Greek DPA clarified that the validity of the identity cards is not in question, but nevertheless it emphasised that the national legal framework concerning the content of the new type of identity cards for Greek citizens should be updated and codified.

3.6.13 HUNGARY

In 2024, the Hungarian DPA issued fines for a total of €853.788. Three cases are presented below:

Case 1: Record fine levied on the public education informatics system operator (eKréta)

eKréta is a software development and advisory organisation, dealing with the public education IT system (KRÉTA system). The databases of the KRÉTA system contain personal data of all students, parents and teachers, i.e. approximately 47 million data in the case of students, 7.5 million in the case of parents and 6.5 million in the case of teachers. eKréta is the data processor concerning the operation of the KRÉTA system. eKréta received notifications from several institutions, according to which those institutions' employees received a message with a malicious code link from the KRETA system. During the investigation of those notifications, one of eKréta's employees opened an infected element and as a result, eKréta became the victim of a phishing attack. The concerned employee's passwords and entry codes were changed, access permissions were deactivated, and the employee's computer was disconnected from the network and replaced. Thereafter eKréta closed the case. However, the concerned employee's login data were synchronised to his Google account, so the hacker remained in the internal systems through an open session. eKréta learnt about the continued existence of the attack and the possibility of a data breach only months later, following a message from the hacker on the internal communication platform. eKréta launched the notification of the data breach to the HU DPA only three days later.

The HU DPA learnt about the data breach from the media on the same day when the hacker sent the message to eKréta on the internal communication platform. The Authority launched and ex officio inspection, which was turned into an ex officio authority procedure following the subsequent media reports and the data breach notification. During the procedure, an on-site inspection was carried out at eKréta's Head office, and an IT expert opinion was prepared. As a result, the HU DPA levied on the data processor a fine of HUF 110 million (ca. €275.000) and won the subsequent Court case, in which the Court fully approved the Authority's decision.

Case 2: Irregular data processing of citizens'IDs in a large-scale energy efficiency programme

The data controller launched a countrywide LED exchange programme advertised to the general public under the energy efficiency obligation scheme. The programme targeted households i.e. natural persons. Under the programme, following an online registration and the conclusion of an energy efficiency agreement, applicants were entitled to LEDs free of charge to exchange their old bulbs in their households to new, modern LED light sources. In order to register to the database, natural persons had to submit their personal data and, in addition, they had to upload both sides of their identity card and the card certifying their address. Most data collected were not necessary and appropriate for the purpose of data processing. At the same time, the data protection notice contained false data and was not easily accessible, while the relevant information of the data processing was incorporated in the general terms and conditions forming part of the concluded energy efficiency agreement. Moreover, the information therein concerning the rights of the data subjects were contrary to the GDPR. In addition, there was no technical solution in place to avoid downloading applicants' collected personal and it was not clear whether inactive users/former employees still had access to the database. The data controller intended to keep the collected personal data for an unlimited period of time, but permanently deleted the data earlier marked for deletion during the procedure.

The HU DPA ordered the data controller to align its data processing activities with the laws and levied a fine of HUF 75 million (ca. €187.500). The data controller contested the Authority's decision, and currently the case is pending before the court.

Case 3: CCTV overseeing employees in a McDonald's restaurant

The HU DPA received a complaint stating that in a McDonald's restaurant the CCTV surveillance system stored recordings for more than two weeks. Moreover sound recording was also taking place in addition to live video recording. Senior managers shared recordings of employees with each other in Messenger groups. According to the complaint, the employees were not informed about the CCTV surveillance and their consent was not requested. The HU DPA investigated the statements in the complaint and carried out an on-site visit at the concerned restaurant. It was established that the rest area of the restaurant designated for the employees during their break was under continuous camera surveillance and that there is no uniform and easily accessible information for employees available about the data processing. In addition, the storage period of the camera footage was not proportionate to the purpose of the data processing. As a consequence, the HU DPA called on the restaurant to align its data processing with the laws and levied a penalty of HUF 30 million (ca. €75.000).

3.6.14 ICELAND

In 2024, the Icelandic DPA performed 14 investigations, received 116 complaints, issued seven compliance orders and adopted one sanction corresponding to approximately €9.961 of fines. Two cases are presented in the following section:

Case 1: In a national case, the Icelandic DPA imposed an administrative fine of approximately €9.961 against a private organisation, Stjarnan ehf., and ordered the organisation to take corrective measures.

The case concerned the use of surveillance cameras at the complainant's workplace. The data controller argued that the organisation had legitimate interests in processing the personal data and that it was necessary for security and asset protection purposes. The investigation revealed that at the time in question, the complainant's supervisor viewed the footage of the surveillance camera at the workplace on two occasions, took screenshots and noted comments on the complainant's procedures and behaviour at work.

The Icelandic DPA found the data controller did not demonstrate the necessity for such extensive processing of personal data and therefore the processing was in breach of Art. 5(1)(a) GDPR, Art. 5(1)(b) GDPR, Art. 5(2) GDPR and Art. 6(1) GDPR, as well as Art. 9 GDPR and Art. 14(1) of the Icelandic Act no. 90/2018, on Data Protection and the Processing of Personal Data.

Case 2: In a cross-border case the Icelandic DPA conducted an audit of the processing of personal data by the organisation SidekickHealth ehf. The Icelandic DPA was the LSA. Bulgaria, Finland, Germany, Italy, Luxembourg, Norway, Spain, and Sweden were CSA's.

The main activity of SidekickHealth is the operation of the mobile application Sidekick. It allows users to record data regarding their health status and subsequently receive feedback. SidekickHealth uses Google as a data processor.

The Icelandic DPA concluded that the processing agreement between SidekickHealth ehf. and Google Ireland Ltd did not comply with the first sentence of Art. 28(3) GDPR and Art. 28(3)(a) GDPR and Art. 25(3) of the Icelandic Act no. 90/2018, on Data Protection and the Processing of Personal Data. The Icelandic DPA also concluded that SidekickHealth ehf. did not take adequate measures for the transfer of personal data to third countries, allowed by a processing agreement with Google Ireland Ltd, in accordance with Art. 44 GDPR. SidekickHealth was therefore reprimanded.

3.6.15 ITALY

In 2024, the Italian DPA performed investigations into several thousands of cases. It also received 4.032 complaints and issued over 230 compliance orders. The Garante adopted over 140 sanctions corresponding to €145.332.449 of fines, relating, among others, infringements of data subject rights, unlawful telemarketing, and data breaches affecting public and private bodies.

Three cases are presented in this section.

Case 1: The Italian DPA took corrective and sanctioning measures against OpenAI in relation to the management of the ChatGPT service. OpenAI will have to carry out a six-month information campaign and pay a fine of €15 million. The Garante forwarded the procedural documents to the Irish DPA, which became LSA on 15 February 2024, in order to investigate any ongoing infringements that have not been exhausted before OpenAI had its establishment in Ireland.

Case 2: The Garante ordered Foodinho S.r.l., an organisation of the Glovo Group, to pay a fine of €5 million for unlawfully processing the personal data of more than 35.000 riders through the digital platform. The Italian DPA also issued specific requirements and prohibited further processing of biometric data (facial recognition) of riders used for identity verification.

Case 3: The Garante ordered an energy organisation to pay a fine of €5 million for serious breaches found in the processing of personal data of more than 2.300 customers in the supply of electricity and gas. The Italian DPA took action following numerous reports and complaints regarding the closing of unsolicited contracts, filled with inaccurate and outdated data of the organisation's customers.

3.6.16 IRELAND

In 2024, the Irish DPA commenced 11 inquiries, received 2.673 complaints, issued five compliance orders and adopted seven decisions corresponding to €652 million of fines. These related, among other things, to personal data breaches concerning the storage of user passwords in plaintext, processing of personal data for the purposes of behavioural analysis and targeted advertising and exploitation by unauthorised third parties of user tokens.

Three cases are presented in this section:

Case 1: Mediahuis Ireland Group Ltd (formerly Irish News and Media plc)

Date of decision: 7 June 2024

The DPC has completed a complaint based national inquiry into Mediahuis Ireland Group Ltd (MIG) processing of personal data in relation to a series of news reports in the print and online editions of three Irish newspapers. The purpose of the inquiry was to examine if any obligations on the data controller arising under Art. 5(1)(a) GDPR, Art. 5(1)(c) GDPR, Art. 5(2) GDPR, Art. 6 GDPR and Art. 9 GDPR had been engaged and, if engaged, whether MIG infringed those obligations in publishing the personal data relating to the complainant as contained in the relevant newspaper articles.

Having regard to the totality of the evidence before it, the DPC found that the exemption under section 43(1) of the

Data Protection Act 2018 applies to the reporting by MIG about which complaint was made by the complainant, and the DPC therefore dismissed the complaint under section 112(1)(b) of the Data Protection Act 2018.

For more information, you can read the summary of the inquiry at this link: Inquiry concerning Mediahuis Ireland Group Limited (MIG) - June 2024

Case 2:Inquiry into Meta Platforms Ireland Limited

Date of Decision: 26 September 2024

This inquiry was launched in April 2019, after Meta Platforms Ireland Limited (MPIL) notified the DPC that it had inadvertently stored certain passwords of social media users in 'plaintext' on its internal systems (i.e. without cryptographic protection or encryption).

The DPC's Decision recorded the following findings of infringement of the GDPR:

- Art. 33(1) GDPR, as MPIL failed to notify the DPC of a personal data breach concerning storage of user passwords in plaintext;
- Art. 33(5) GDPR, as MPIL failed to document personal data breaches concerning the storage of user passwords in plaintext;
- Art. 5(1)(f) GDPR, as MPIL did not use appropriate technical or organisational measures to ensure appropriate security of users' passwords against unauthorised processing; and
- Art. 32(1) GDPR, because MPIL did not implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality of user passwords.

The decision included a reprimand and administrative fines totalling €91 million.

For more information, you can download the full decision at this link: Inquiry into Meta Platforms Ireland Limited - September 2024 (PDF, 1.2 MB).

Case 3: LinkedIn Ireland Unlimited Company Decision

Date of Decision: 22 October 2024

The inquiry examined LinkedIn's processing of personal data for the purposes of behavioural analysis and targeted advertising of users who have created LinkedIn profiles (members). This inquiry was launched by the DPC, in its role as the Data Protection Authority that is in the lead, called the Lead Supervisory Authority (LSA) for LinkedIn, following a complaint initially made to the French DPA.

The DPC's final decision recorded the following findings of infringement of the GDPR:

- Art. 6 GDPR and Art. 5(1)(a) GDPR, insofar as it requires the processing of personal data to be lawful, as LinkedIn;
- Art. 13(1)(c) GDPR and Art. 14(1)(c) GDPR, in respect of the information LinkedIn provided to data subjects regarding its reliance on Art. 6(1)(a) GDPR, Art. 6(1)(b) GDPR and Art. 6(1)(f) GDPR as lawful bases;
- Art. 5(1)(a) GDPR, the principle of fairness.

The decision included a reprimand, an order for LinkedIn to bring its processing into compliance, and administrative fines totalling €310 million.

For more information, you can download the full decision at this link: Inquiry into LinkedIn Ireland Unlimited Company - October 2024 (PDF, 1.8 MB).

3.6.17 LATVIA

In 2024, the Latvian DPA performed 974 investigations, received 693 complaints, issued 26 compliance orders and adopted 14 sanctions corresponding to €6.150 of fines relating. Two cases are presented in this section.

Case 1: The National Electronic Mass Media Council (NEPLP) published an administrative penalty decision on its website, which included the name, surname, and personal identification number of a data subject. The published decision made sensitive personal data accessible to the public, violating the GDPR.

The Data State Inspectorate found that the personal identification number had been published due to an error, and NEPLP quickly removed it. However, the name and surname remained accessible on the website. NEPLP explained that the purpose of publishing decisions was to inform industry representatives and promote understanding of regulatory requirements. The Inspectorate determined that achieving these goals did not require the publication of personal data.

The Inspectorate concluded that NEPLP had violated data processing principles and required it to delete all personal data from the published decisions by a specified deadline.

Case 2: A physician assistant, using authorised access to unified health information systems, including E-Health and other information systems containing health data of individuals, unlawfully processed the personal data of several individuals. The data processing was conducted for personal purposes and was unrelated to the performance of work duties, thereby violating the GDPR and the principle of confidentiality.

The violation involved the processing of sensitive data without a legal basis, causing emotional distress to the affected individuals. The medical institution confirmed that the employee's actions were inconsistent with professional standards and legal regulations. Consequently, the employee was fined €500, considering the severity of the violation and its impact on the affected individuals.

Link to annual reports of Latvian DPA: https://www.dvi.gov.lv/lv/publikacijas-un-parskati

3.6.18 LIECHTENSTEIN

In 2024, the Liechtenstein DPA conducted nine investigations, processed 50 complaints, issued nine compliance orders, and imposed three sanctions, resulting in fines totalling €22.911. These sanctions primarily addressed issues such as transparency obligations, a data breach involving special categories of personal data, and violations of data subject rights.

Two cases are presented in this section.

Case 1: A former employee filed a complaint related to Art. 15 GDPR, claiming he was granted access only to his file, which included most of his work-related documents. However, specific data appeared to be missing from the file.

The DPA clarified that a data controller must also comply with the requirements outlined in Art. 15(1) GDPR. This entails providing the data subject with all the specified information, such as the purpose of the processing, the recipients, the data retention period, and other elements listed in paragraph 1. While providing access to a digital file may satisfy the requirements of Art. 15(3) GDPR, it does not fulfil the obligations under paragraph 1.

Additionally, the data controller cited Art. 34 of the National Data Protection Act, arguing that the data was stored solely for data security and control. However, even if the data controller relies on this exception, they must inform the data subject that they are invoking the exception.

Case 2: An online health advisory service provider unintentionally exposed users' and employees' email addresses and phone numbers online due to a technical error. The organisation attributed the breach to incorrect access rights configuration.

The DPA stated that the unprotected access to sensitive data violated Art. 32 GDPR, as it compromised data confidentiality and integrity. Furthermore, the data controller was notified of the breach by an anonymous individual but failed to act or verify the report, thus constituting a violation of Art. 33 GDPR. A fine was subsequently imposed.

3.6.19 LITHUANIA

In 2024, the Lithuanian DPA imposed 13 sanction, resulting in fines up to €2.423.971. Three cases are presented in this section.

Case 1: On July 3, 2024, the Inspectorate imposed a fine of €2.3 million on online marketplace for buying, selling, and exchanging new or second-hand items. The decision followed an investigation that revealed significant violations of key GDPR principles, particularly transparency, fairness, and accountability. Specifically, it was found that the organisation: 1) Failed to adequately address data subjects' requests for erasure and provided insufficient information, violating Art. 5(1)(a) GDPR, Art. 12(1) GDPR, and Art. 12(4) GDPR; 2) Neglected to properly implement the accountability principle, breaching Art. 5(2) GDPR; and 3) Engaged in unlawful data processing practices in the context of shadow banning, violating Art. 5(1)(a) GDPR and Art. 6(1) GDPR.

Case 2: On September 19, 2024, the Inspectorate imposed a €6.000 fine on an organisation providing dental healthcare services following an investigation into a complaint. The examination revealed that the organisation violated the principle of lawfulness under Art. 5(1) GDPR by conducting video and sound surveillance within dental offices without proper legal grounds. Additionally, the organisation infringed upon the complainant's right of access under Art. 15(3) GDPR by refusing to provide the copy of the processed data upon his request.

Case 3: In 2024, the Inspectorate investigated a complaint regarding GDPR violations by an organisation managing an online database of used vehicle records. The inquiry determined that the Organisation had breached Art. 5(1) GDPR, Art. 15(1) GDPR, and Art. 16 GDPR by failing to ensure the accuracy of personal data, denying access to requested information, and unlawfully refusing to rectify inaccurate data. The Inspectorate upheld the complaint, issued a reprimand, and directed the Organisation to resolve the identified violations within a specified timeframe. However, due to the improper execution of these instructions, the Inspectorate imposed a fine of €12.000 to the organisation on November 28, 2024, for breaching Art. 58(2) GDPR.

All of the aforementioned decisions are being contested before the regional administrative court.

3.6.20 LUXEMBOURG

In 2024, the Luxembourgish DPA performed 29 investigations, received 516 complaints, issued two compliance orders including one sanction corresponding to a fine of €2.300. These two decisions relate to video surveillance systems in the workplace.

Two cases worth highlighting are presented in this section.

Case 1: The first case was based on a complaint of a data subject who was of the opinion that their employer (a municipality) violated certain provisions of the GDPR because their employer used data collected through a video surveillance system to justify the termination of their employment contract. The Luxembourgish DPA concluded that the data controller did in fact violate Art. 5(1)(b) GDPR (principle of purpose limitation) and therefore issued a reprimand to the data controller without other corrective measures. The Luxembourgish DPA does not have the power to fine the State and the municipalities in Luxembourg.

Case 2: In the second case, the Luxembourgish DPA carried out an on-site investigation in the offices of a data controller (a small private organisation) in order to find out if their video surveillance system was in compliance with the provisions of the GDPR and the national data protection law of 1 August 2018. The Luxembourgish DPA concluded that the data controller infringed several provisions of the GDPR, namely Art. (6)(1) GDPR (lawfulness of processing), Art. 5(1)(a) GDPR (principle of transparency) linked to Art. 13(1) GDPR and 13(2) GDPR (information to be provided to data subjects), Art. 5(2) GDPR (accountability principle) linked to Art. 24(1) GDPR (responsibility of the data controller), Art. 5(1)(e) GDPR (storage limitation principle) and Art. 32(1) GDPR (security of processing).

It therefore imposed a definitive limitation on processing according to Art. 58(2)(f) GDPR concerning the data processed by two specific cameras and an order to bring processing operations into compliance with Art. 5(1)(a) GDPR linked to Art. 13(1) GDPR and Art. 13(2) GDPR according to Art. 58(2)(d) GDPR. In addition to the aforementioned measures, the Luxembourgish DPA also imposed a fine of €2.300 on the data controller.

Link to annual report: https://cnpd.public.lu/en/publications/rapports.html

3.6.21 MALTA

In 2024, the Maltese DPA performed 793 investigations, received 882 local complaints and acted as LSA for 256 cross-border complaints, issued 112 compliance orders and adopted three sanctions corresponding to €18.000 of fines.

Two cases are worth highlighting.

Case 1: The Maltese DPA fined a private organisation €15.000 for contacting the data subject through two direct and unsolicited marketing calls. This occurred despite the organisation confirming, following a previous complaint, that the data subject's personal data undergoing processing for direct marketing purposes had been erased and her mobile numbers were barred from the internal systems.

The investigation found that the data controller's centralised telephone system had a feature to suppress all outgoing calls marked as 'do not call back'. While this measure was deemed appropriate, sub-contracted individuals bypassed the system as instead they were using personal mobiles to make calls. As a result, the data subject's mobile numbers were contacted again after being randomly generated by the software, despite her previous objection.

The DPA found the data controller was in breach of Art. 21(2) GDPR for failing to instruct its sub-contracted individuals and for not taking adequate steps to respect the data subject's rights.

Case 2: The Maltese DPA decided that the data controller infringed the principle of fairness and the national legislation transposing Art. 13 of the LED, by failing to inform individuals that they are approaching a zone monitored by hand-held speed cameras.

The DPA ordered the data controller to display appropriate signs that must be positioned within a reasonable distance and in such a manner that the data subject could easily recognise the circumstances of the processing before approaching a zone where hand-held speed devices are used.

3.6.22 NETHERLANDS

In 2024, the Dutch DPA performed 22 investigations, handled 6.232 complaints, issued nine compliance orders and adopted 16 sanctions corresponding to €328million of fines. These relate among other, to international transfers without meeting the requirements of the GDPR to ensure the necessary level of protection, and to processing personal data without a legal basis to do so. Two cases are highlighted in the following section:

Case 1: The Dutch Data DPA imposed a fine of €290 million on Uber. The Dutch DPA found that Uber transferred personal data of European taxi drivers to the United States (US) and failed to appropriately safeguard the data with regard to these transfers. According to the Dutch DPA, this constitutes a serious violation of the GDPR. In the meantime, Uber has ended the violation.

Case 2: The Dutch DPA imposed a fine of €30.5 million and orders to end the still ongoing violations subject to a non-compliance penalty of a maximum of €5.1 million. Clearview is an American organisation that offers facial recognition services. Among other things, Clearview has built an illegal database with billions of photos of faces, including of Dutch people. The Dutch DPA warned that using the services of Clearview is also prohibited.

3.6.23 NORWAY

In 2024, the Norwegian DPA performed 18 investigations, received 902 complaints, issued 28 compliance orders and adopted four sanctions corresponding to approximately €63.000 of fines. These relate, among other, to a data breach involving sensitive information and a failure to meet the GDPR requirements on securing personal data. Two cases are presented below:

Case 1: In a national case, the Norwegian DPA imposed an administrative fine of approximately €21.500 to a municipality for violating the GDPR after confidential personal data was unintentionally made accessible in public records. The breach involved sensitive information about students, including their names, birth dates, national ID numbers, and personal details. Although the municipality reported the breach and took corrective action, the Norwegian DPA determined that they failed to meet adequate requirements of the GDPR regarding security and legal basis.

Case 2: In a national case, the Norwegian DPA imposed an administrative fine of approximately €13.000 to a university for violating the GDPR by failing to secure personal data in Microsoft Teams. A data breach that was discovered revealed that personal data from 16.000 individuals, including employees, students, and refugees, had been exposed in open Teams folders since 2018. The breach included sensitive information such as names, ID numbers, and exam details. Following the case, the university was obliged to improve procedures, ensure proper data access controls, and provide training to employees on safeguarding personal data.

3.6.24 POLAND

In 2024, the Polish DPA performed 41 investigations, received 8.056 complaints, issued 334 compliance orders and adopted 25 sanctions corresponding to €2.9 million of fines relating.

There are three cases worth highlighting presented in this section.

Case 1: The Polish DPA fined mBank over PLN 4 million (€900.000) for failing to notify customers of a data breach. On June 30, 2022, an employee of a data processing organisation mistakenly sent client documents to another financial institution. The opened envelope raised concerns about unauthorised access to sensitive data, including personal details, bank account information, and income data.

Although mBank reported the incident to Polish DPA, it did not inform affected individuals, arguing the recipient was trustworthy. Polish DPA rejected this reasoning, stressing that trustworthiness requires a well-established, long-term relationship. The breach created significant risks to individuals, leaving them unable to protect themselves. The fine highlights mBank's systemic failure to meet the GDPR obligations.

Case 2: During a press conference, prosecutors revealed personal data of a victim in a criminal case, including sensitive information protected under the GDPR. Despite this breach, the Prosecutor's Office neither reported the incident to the Polish DPA nor informed the individual, arguing the data was part of a court ruling and disclosed within legal obligations. The Polish DPA disagreed, emphasising that even public entities must comply with the GDPR.

The President of the Personal Data Protection Office imposed a fine of €19.800 for infringements of Art. 6, 33 and 34 of the GDPR on the National Public Prosecutor's Office. In addition, he ordered the National Public Prosecutor's Office to notify the victim, in accordance with the GDPR, of the possible consequences of the breach and of the measures, applied or proposed by the controller, to minimise the effects of the breach.

The President of the Personal Data Protection Office in Poland noted the lack of legal grounds for such disclosure and stressed the importance of protecting victim data, particularly given the role of the Prosecutor's Office in upholding the law. The fine underscores the need for strict compliance with data protection regulations.

Case 3: The President of the Personal Data Protection Office imposed a fine of PLN 10.913 (€2.500) on the "Stop LGBT" Legislative Initiative Committee for violating data protection rules during a signature collection campaign. Support lists containing sensitive data, such as names, surnames, ID numbers, and addresses, were left unsecured in a church.

The Polish DPA investigation revealed flaws in risk assessment and a lack of oversight over the data. The lists were publicly accessible, allowing them to be viewed, copied, or photographed. The administrator failed to foresee the risk of exposing the data to third parties and did not implement effective protective measures.

The committee attributed the situation to the spontaneity of the process. However, the Polish DPA President concluded that neglecting the GDPR obligations exposed the data to risks. The committee was instructed to notify affected individuals of the breach and implement proper safeguards.

3.6.25 PORTUGAL

In 2024, the Portuguese DPA started 1.670 investigations procedures, performed 21 inspections, received 1.221 complaints, issued one compliance order, issued 151 warnings and applied 23 fines in the amount of €138.375.

Under the GDPR only, 12 sanctions where adopted, corresponding to €88.375 of fines. These relate, among other, to the exercise of data subjects' rights, to the lawfulness of processing, to transparency obligations and to the lack of designation of a DPO.

Two cases are presented in this section.

Case 1: Following media reports of Worldcoin Foundation's activities in Portugal, the PT DPA conducted an inspection on the collection of biometric data in specific pop-up kiosks operated by its data processor, Tools for Humanity. Subsequently, the PT DPA publicly advised to carefully consider the implications before providing their biometric data. Due to a growing number of complaints, particularly regarding the collection of minors' data, without parental consent, the impossibility of deleting data and concerns about potential uses of the data, the PT DPA issued an order to the data controller to suspend the biometric data collection within Portugal, in order to safeguard the fundamental right to personal data protection, especially for minors. Worldcoin Foundation, now known as World, has not resumed operations in Portugal. After receiving information regarding the existence of an establishment of Worldcoin Foundation in Germany, the Procedure was sent to the Bavarian Authority (BayLDA).

Case 2: Following the EDPB Opinion 11/2024 on facial recognition for streamlining airport passenger flow, the PT DPA conducted an inspection at Lisbon's Humberto Delgado Airport. A team of three auditors examined the associated data processing activities, hardware, and use cases involving biometric data. To analyse thoroughly the "Biometric Experience," this assessment was performed in a laboratory setting at the data controller's facilities, ANA Aeroportos. The data controller provided satisfactory responses to inquiries and demonstrated all relevant business cases. The inspection findings have been documented and are currently undergoing legal review for the GDPR compliance.

Link to annual report of PT DPA:
https://www.cnpd.pt/cnpd/relatorios-de-atividades/

3.6.26 ROMANIA

Case 1: The data controller for Bucharest Municipality District 1 has been fined RON 159.000 for failing to comply with a remedial order issued by the Romanian DPA. The investigation began following concerns about potential violations of data processing laws involving an online platform used to collect personal data.

Initially, District 1 received a reprimand for not providing the requested information. A remedial plan was issued, requiring the submission of the requested data within ten days. However, when the municipality failed to comply, the DPA imposed a RON 10.000 fine.

Despite the second report's warning, the district again failed to provide the required information, leading to the imposition of a coercive fine of RON 159.000. This fine was calculated for a 53-day delay (from December 29, 2023, to February 19, 2024). Under Law no. 102/2005, the DPA is authorized to fine up to RON 3.000 for each day of delay if a data controller fails to meet an ordered corrective measure or refuses to cooperate during an investigation.

Case 2: In October 2024, the Romanian DPA completed an investigation into data controller Altex România S.A. and found violations of the provisions of Art. 32 (1)(b) GDPR and of Art. 32 (2) GDPR. The data controller was sanctioned with a fine of RON 99.516.

The investigation followed two personal data breach notifications from Altex România:

- The data controller was informed by e-mail by a third party about the fact that some accounts of the data controller's customers were published on a platform, and that the personal data of a very large number of data subjects being affected, namely: name, surname, e-mail, altex.ro account's password, information available in the customer account, such as delivery address, telephone number, order history, data related to the cards with which the online payment is made, communications in connection with the data controller;
- The data controller reported a "credential stuffing" computer attack, through repeated attempts to validate passwords on some customer accounts for placing gift cards orders; the following personal data were affected, for a significant number of data subjects: name, surname, e-mail address, customer account access password, and registered bank cards in the app/website.

The Romanian DPA found that Altex România S.A. did not implement adequate security measures. This led to the unauthorised access to the personal data of a very large number of customers.

In addition to the fine, the DPA ordered corrective measures to improve security of the processing, namely, by changing the login notification, displaying the logged in devices in the account, changing the password policy, and implementing measures to monitor the incoming and outgoing internet traffic.

Case 3: Following a complaint, the Romanian DPA found that a controller disclosed the e-mail addresses of individuals when information was distributed by email, because the recipients' addresses were not included in 'blind car-

bon copy' (BCC). This led to the disclosure of approximately 180 e-mail addresses to other recipients, thus infringing the obligations imposed by Art. 32 GDPR.

A fine of RON 24.870,5 was imposed (the equivalent of €5.000) together with the corrective measure of re-evaluation of the implemented security measures, so as to ensure a level of security adequate to the risk of the processing, especially in terms of training the persons who process data under the authority of the controller and the regular verification of compliance with the instructions sent to them.

3.6.27 SLOVENIA

In 2024, the Slovenian DPA performed 384 investigations, received 184 complaints, issued 25 compliance orders and adopted five sanctions under the GDPR, corresponding to €51.000 of fines.

These relate[11] to data processing without an appropriate legal basis and inadequate security of processing according to Art. 32 GDPR.

There are three cases worth highlighting which are presented in this section.

Case 1: The Slovenian DPA carried out an infringement procedure against the organisation FOVELLA d.o.o., acting as the owner of DODO PIZZA franchise in Slovenia. The DPA had previously found two breaches in the inspection proceeding, relating to unlawful CCTV inside working premises and live broadcast of these CCTV footages on the organisation's website. The Slovenian DPA decided that there is no legal basis under national legislation and Art. 6 GDPR for specific CCTV. The Slovenian DPA imposed a fine of €25.000 to the organisation for unlawful CCTV inside working premises and the broadcast of the footages via the organisation's website. The DPA also issued a reprimand for breach of national Data Protection Act and Art. 13 GDPR, as the organisation failed to inform data subjects of the data processing.

Case 2: The Slovenian DPA assessed the lawfulness of video surveillance in a primary school. It was established that the data controller was unlawfully recording the school lobby and the corridor and published an incomplete notice on the processing of personal data according to national Data Protection Law and Art. 13 GDPR. Following a notice from the DPA, the data controller re-directed the cameras to only cover the entrance to the school, as allowed by the national law, and updated the notice on the processing of the personal data.

Case 3: The Slovenian DPA received a complaint from an individual regarding the erasure of his personal data from criminal records, as the data retention period had expired. The police rejected his request and explained that Police Tasks and Powers Act provides, that after the expiry of retention periods, the criminal records data shall be blocked, and the data shall be retained for 30 years. The DPA found that a constitutional review was required to determine whether the retention period of blocked data and the method of anonymisation after the expiry of the retention period were set appropriately and whether the principles of purpose limitation, data minimisation and limitation of the retention period were respected. The Slovenian DPA has therefore suspended the proceedings and submitted a request for a review of the constitutionality and legality to the Constitutional Court.

Link to annual report of the Slovenian DPA:
https://www.ip-rs.si/publikacije/letna-poro%C4%8Dila/

3.6.28 SPAIN

In 2024, the Spanish DPA performed 311 investigations, received 18.841 complaints, issued 391 compliance orders and adopted 281 sanctions corresponding to about €35.6 million of fines. These relate among other, to fraud in service contracts, personal data breaches concerning large companies such as insurance, energy suppliers or telecoms. The fines concern both data protection by design and lack of measures to ensure an appropriate level of security, but also the non-compliance of data protection principles, for example the lawfulness of the processing of banks and telecoms; or the processing of special categories of personal data such as health records by employers.

Three cases are presented in this section, representative of these topics and sectors.

Case 1: PS/00216/2023

The Spanish DPA imposed a find of €5 million on the electricity company Energya VM Gestión de Energía S.L. The company was fined €2.5 million for infringements of Art. 5(1)(a) GDPR (lack of fairness and transparency) and €2.5 million for infringements of Art. 5(2) GDPR.This procedure initiated after the Spanish DPA received complaints from customers of another electricity company (Naturgy), allegedly on behalf of their current electricity company. The controller deceived individuals to attract customers, and modify the data of the individuals in the databases of Naturgy.

11 This data refers only to the GDPR, however the SI DPA also conducts proceedings and imposes measures and sanctions for infringements of the Data protection Act (ZVOP-2) and Act on the Protection of Personal Data in the Field of Criminal Offences (ZVOPOKD). Most of the infringements in these proceedings concern, among other, unlawful disclosure of personal data to unauthorised users, unlawful publication of personal data, unlawful collection of personal data, unlawful video surveillance and unlawful processing in direct marketing activities.

Case 2: PS/00145/2023

The procedure was initiated by the personal data breach suffered in a web application of the electricity distribution organisation I-DE Redes Eléctricas S.A., belonging to the Iberdrola Group.

The breach was caused by a computer attack exploiting a vulnerability in the I-DE web application and affected the confidentiality of 1.35 million I-DE customers.

A fine of €2.5 million was imposed for the infringement of Art. 5(1)(f) GDPR and another one of €1 million for infringement of Art. 32 GDPR.

The breach also affected almost 2 million customers of two other companies of the Group, as the attacker managed to violate the logical separation existing in the common database of the entities of the Iberdrola Group.

Case 3: PS/00291/2023

In the telecommunications sector, a number of important sanctioning procedures have also been carried out, such as PS/00291/2023 against Telefónica de España SAU. This case was opened as a result of the notification of a personal data confidentiality breach, in which the data affected were landline telephone numbers and equipment data of more than 1.4 million customers.

The breach occurred as a result of massive access (from 55.000 requests a day to 4 million requests and by a single user), through a web portal used by employees to access customer data.

Telefónica was sanctioned €500.000 and €800.000 for violations of Art. 5(1)(f) GDPR and Art. 32 GDPR.

Link to annual report: Memorias | AEPD

3.6.29 SWEDEN

In 2024, the Swedish DPA (Integritetsskyddsmyndigheten, IMY) performed 418 investigations, received 3.814 complaints, issued 23 compliance orders and adopted six sanctions corresponding to €5.2 million of fines relating. Two cases are presented in this section.

Case1: Wrongful use of Meta Pixel

After receiving a data breach notification from a Swedish digital bank, IMY launched an investigation. The breach concerned the banks' use of the Meta Pixel on its web site and app. The Meta Pixel was used to optimise the banks' marketing on Facebook. By mistake, the bank had activated functions in the Meta Pixel, which meant that personal data, such as account numbers and securities, had been transferred erroneously to Meta. IMY concluded that the bank had processed personal data in violation of Art. 5(1)(f) GDPR and 32(1) GDPR by failing to take appropriate technical and organisational measures to ensure an appropriate level of security for the personal data in question when using the Meta Pixel. IMY issued a fine of approximately €1.3 million against the bank.

During 2024, IMY has carried out several additional investigations into other organisations using the Meta Pixel. Some of these have also ended up with IMY issuing fines.

Case 2: Unauthorised camera surveillance by housing organisation

After receiving a complaint, IMY launched an investigation of a housing organisation and its use of camera surveillance in an apartment building. In the building, there were cameras in the entrances to three stairwells and a basement entrance to the property. There were also several cameras in the basement, storage room, operations, laundry room, garbage room, garage and corridors to the sites. IMY found that the organisation had processed personal data in violation of Art. 6(1) GDPR and Art. 13 GDPR by conducting camera surveillance in the apartment building without proper legal basis. IMY ordered the organisation to cease all camera surveillance in the apartment building, except for the parking garage, and issued a fine of €17.375 against the organisation.

4. ANNEXES

This chapter gathers documents, opinions, and tools developed or adopted in 2024 by the EDPB. These annexes serve as a detailed reference for stakeholders and DPAs, illustrating the breadth of the Board's work in clarifying the GDPR and supporting consistent enforcement across the EU.

4.1 GENERAL GUIDANCE ADOPTED IN 2024

Guidelines adopted prior to public consultation

- Guidelines 01/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR – Adopted on 8 October 2024;
- Guidelines 02/2024 on Article 48 GDPR – Adopted on 2 December 2024.

Guidelines adopted after public consultation

- Guidelines 01/2023 on Article 37 of the Law Enforcement Directive (LED) – Adopted on 19 June 2024;
- Guidelines 02/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive – Adopted on 7 October 2024.

4.2 CONSISTENCY OPINIONS ADOPTED IN 2024

4.2.1 Art. 64(1) GDPR Opinions

Draft codes of conduct

- Opinion 12/2024 on the draft decision of the French Supervisory Authority regarding the "Code of Conduct for Service Providers in Clinical Research" submitted by EUCROF – Adopted: 18 June 2024.

Accreditation standards for certification bodies and schemes

- Opinion 7/2024 on the draft decision of the German North Rhine-Westphalia Supervisory Authority regarding the EU Cloud Service Data Protection (Auditor) certification criteria – Adopted: 17 April 2024;
- Opinion 10/2024 on the draft decision of the competent supervisory authority of Sweden regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 GDPR – Adopted: 23 May 2024;
- Opinion 18/2024 on the draft decision of the Austrian Supervisory Authority regarding DSGVO-zt GmbH certification criteria – Adopted: 16 July 2024;
- Opinion 26/2024 on the draft decision of the DE Bremen Supervisory Authority regarding the "Catalogue of Criteria for the Certification of IT-supported processing of Personal Data pursuant to art 42 GDPR ('GDPR – information privacy standard')" presented – Adopted: 2 December 2024.

Approvals of Binding Corporate Rules (BCRs)

- Opinion 01/2024 on the draft decision of the Dutch Supervisory Authority regarding the Processor Binding Corporate Rules of the Booking.com Group – Adopted: 16 January 2024;
- Opinion 2/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the TELEFÓNICA Group – Adopted: 13 February 2024;
- Opinion 3/2024 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Accenture Group – Adopted: 13 February 2024;
- Opinion 05/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the MAPFRE Group – Adopted: 14 March 2024;
- Opinion 9/2024 on the draft decision of the Romanian Supervisory Authority regarding the Processor Binding Corporate Rules of the Genpact Group – Adopted: 23 May 2024;
- Opinion 13/2024 on the draft decision of the Supervisory Authority of Liechtenstein regarding the Controller Binding Corporate Rules of the Ivoclar Vivadent Group – Adopted: 18 June 2024;
- Opinion 14/2024 on the draft decision of the Estonian Supervisory Authority regarding the Processor Binding Corporate Rules of the Mercans Group – Adopted: 16 July 2024;
- Opinion 15/2024 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the AVATURE Group – Adopted: 16 July 2024;

- Opinion 16/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the AVATURE Group – Adopted: 16 July 2024;
- Opinion 17/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the FCC Group – Adopted: 16 July 2024;
- Opinion 20/2024 on the draft decision of the North Rhine-Westphalian Supervisory Authority regarding the Controller Binding Corporate Rules of the Viega Group – Adopted: 17 September 2024;
- Opinion 21/2024 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the Talan Group – Adopted: 17 September 2024;
- Opinion 23/2024 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Aptiv Group – Adopted: 4 November 2024;
- Opinion 24/2024 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Controller Binding Corporate Rules of the Infosys Group – Adopted: 2 December 2024;
- Opinion 25/2024 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Processor Binding Corporate Rules of the Infosys Group – Adopted: 2 December 2024.

4.2.2 Art. 64(2) GDPR Opinions

- Opinion 04/2024 on the notion of main establishment of a controller in the Union under Art. 4.16(a) GDPR – Adopted: 13 February 2024;
- Opinion 6/2024 on the draft list of the Latvian SA on pro-cessing operations exempt from the data protection impact assessment requirement (Art. 35.5 GDPR) – Adopted: 16 April 2024;
- Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms – Adopted: 17 April 2024;
- Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR) – Adopted: 23 May 2024;
- Opinion 19/2024 on the EuroPrise criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR) – Adopted: 16 July 2024;
- Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s) – Adopted: 7 October 2024;
- Opinion 27/2024 on the Brand Compliance criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR) – Adopted: 2 December 2024;
- Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models – Adopted: 17 December 2024.

4.3 STATEMENTS ON LEGISLATIVE DEVELOPMENTS

- Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse – Adopted: 13 February 2024;
- Statement 2/2024 on the financial data access and payments package – Adopted: 23 May 2024;
- Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework – Adopted: 16 July 2024;
- Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR – Adopted: 7 October 2024;
- Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement – Adopted: 4 November 2024;
- Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation - Fostering Cross-Regulatory Consistency and Cooperation – Adopted: 3 December 2024.

4.4 OTHER DOCUMENTS

Enforcement and Cooperation Tools

Support and Capacity Building - reports commissioned by the EDPB and drafted by SPE experts

- Report on the extraterritorial enforcement of the GDPR
- Report on the use of SPE external experts
- Standardised Messenger Audit

- Data Protection Officer training in Croatia
- AI Risks: Optical Character Recognition and Named Entity Recognition

Taskforces

- ChatGPT Taskforce Report

One-stop-shop case digest - reports commissioned by the EDPB and drafted by SPE experts

- One-stop-shop case digest on right of access

CONTACT DETAILS

Postal address

Rue Wiertz 60, B-1047 Brussels

Office address

Rue Montoyer 30, B-1000 Brussels

An Executive Summary of this report, which provides an overview of key EDPB activities in 2024, is also available. Further details about the EDPB can be found on our website at edpb.europa.eu.