

Clarity in action: Supporting stakeholders through guidance and dialogue

Annual Report 2025

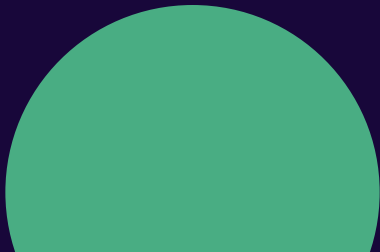
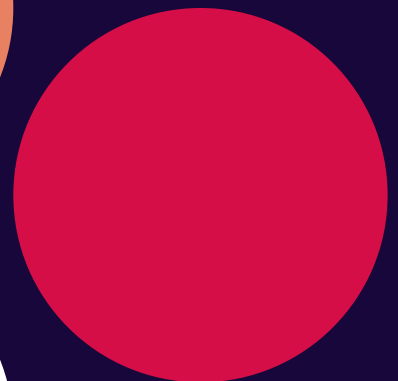
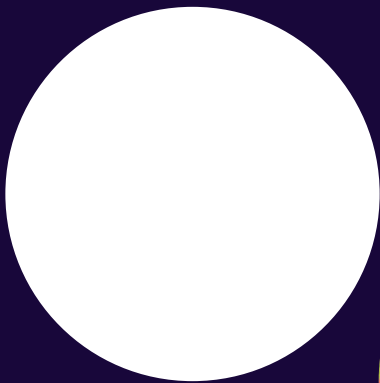
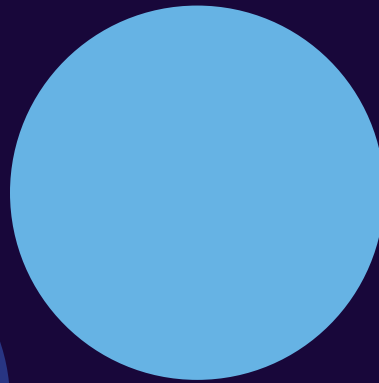
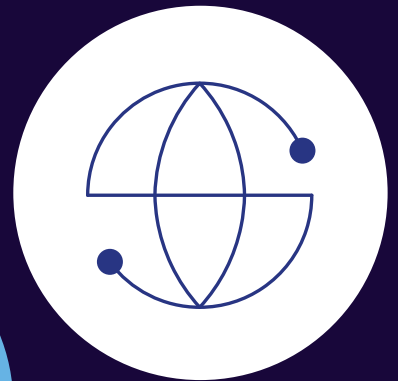


Table of Contents

Foreword	3	3.6.1 Austria	32
Highlights	4	3.6.2. Belgium	32
1. The EDPB Secretariat	6	3.6.3. Bulgaria	32
1.1 Mission And Activities	8	3.6.4. Croatia	33
2. European Data Protection Board – Activities in 2025	12	3.6.5. Cyprus	33
2.1 Bridging Fundamental Rights and Digital Innovation Through GDPR Compliance	12	3.6.6. Czech Republic	33
2.1.1 Helsinki high-level meeting: enhanced clarity, support and engagement	12	3.6.7. Denmark	33
2.1.2 Regulation on procedural rules and Omnibus regulation on the record of processing	14	3.6.8. Estonia	34
2.1.3 Cross regulatory cooperation	14	3.6.9. Finland	34
2.1.4 The EDPB in a global context	15	3.6.10. France	34
2.2 Ensuring Consistent Protection	16	3.6.11. Germany (DPA Berlin)	35
2.2.1 Guidance and Recommendations	16	3.6.12. Germany (DPA Hamburg)	35
2.2.2 Consistency Opinions	18	3.6.13. Germany (Federal DPA)	35
2.2.3 Legislative Consultation	19	3.6.14. Greece	35
2.2.4 Stakeholder Consultation	21	3.6.15. Hungary	35
3. Supporting Enforcement	24	3.6.16. Iceland	36
3.1 EDPB Activities To Support GDPR Enforcement And Cooperation Among DPAs	24	3.6.17. Ireland	36
3.1.1 Coordinated Enforcement Framework	24	3.6.18. Italy	36
3.1.2 Support Pool of Experts	24	3.6.19. Latvia	37
3.1.3 Taskforces	27	3.6.20. Liechtenstein	37
3.2 Litigation	27	3.6.21. Lithuania	37
3.3 Cooperation Under The GDPR	29	3.6.22. Luxembourg	38
3.4 Binding Decisions	29	3.6.23. Malta	38
3.5 National Cases With Exercise Of Corrective Powers	31	3.6.24. Netherlands	39
3.6 Selection Of National Cases	32	3.6.25. Norway	39
		3.6.26. Portugal	39
		3.6.27. Romania	40
		3.6.28. Slovakia	40
		3.6.29. Slovenia	41
		3.6.30. Spain	41
		3.6.31. Sweden	41
		4. Annexes	42
		4.1 General guidance and recommendations	42
		4.2 Consistency opinions	42
		4.3 Legislative consultation	43
		4.4 Other documents	43

Foreword



This year, we have seen the data protection landscape change significantly. The rapid expansion of the EU's digital regulatory framework added complexity to the data protection ecosystem. In a truly cross-regulatory environment where data protection laws intersect with other digital regulations, it is our responsibility as regulator to clarify the interplay between data protection rules and other digital laws, and to ensure legal certainty and consistency.

In 2025, we adopted guidelines on the interplay between the Data Services Act (DSA) and the GDPR, and we adopted our first set of joint guidelines with the European Commission (EC) on the interplay between the Digital Markets Act (DMA) and the GDPR. In addition, we have also worked with the Commission on joint guidelines on the interplay between the AI act and EU data protection laws and will publish these in 2026. This so-called interplay guidance is crucial to provide a single, harmonised reference point, so that organisations understand how the rules fit together and individuals are better protected. By placing fundamental rights at the core of digital transformation, we can ensure that technological progress and European values go hand in hand.

As the regulatory landscape has grown more complex, there is a corresponding demand for regulatory simplification: to support innovation and economic growth, it is important to cut unnecessary administrative burden for business. The EDPB has been actively working to address this while, at the same time, ensure that simplification does not lower the protection of individuals' fundamental rights.

Last July, we took a pivotal step with a high-level meeting organised in my home-town Helsinki, to assess how we can further facilitate compliance, ensure greater regulatory clarity and improve our processes. With this in mind, we adopted the

[Helsinki Statement on Enhanced Clarity, Support, and Engagement](#). The statement outlines new initiatives to make GDPR compliance easier, strengthen consistency, enhance the dialogue and improve transparency with stakeholders and boost cross-regulatory cooperation.

In 2025, we delivered important progress in all fields of the Helsinki initiative. From joint guidelines, seeking input on which templates are useful to organisations, to improved drafting procedures and greater stakeholder engagement.

In parallel to our own efforts to simplify and support compliance, in 2025, the European Commission took further initiative to simplify rules to reduce the administrative burden for organisations through the Digital Omnibus proposal.

The Digital Omnibus launched an important debate on how best to foster innovation through trimming unnecessary regulatory requirements. The EDPB welcomed the discussion on effective digital regulation: we are committed to finding solutions to make GDPR compliance easier, especially for small organisations. At the same time, it is our task, as regulator that simplification does not amount to deregulation and that core data protection rights are safeguarded. We held important discussions on this during our plenary meetings, which will feed into the EDPB and EDPS joint opinions, to be adopted in the first months of 2026.

The EDPB remains committed to guiding organisations and individuals through an evolving regulatory environment, ensuring that the GDPR continues to be a benchmark for privacy and innovation worldwide and a global standard for data protection and digital governance.

Anu Talus

Chair of the European Data Protection Board

Highlights

JANUARY

Guidelines on pseudonymisation

JANUARY

CEF 2024 report on right of access

MARCH

Launch CEF 2025 on the right to erasure

APRIL

Guidelines on blockchain

MAY

Opinion on the Commission's draft adequacy decision regarding the European Patent Organisation (EPO)

JULY

Joint Opinion on the draft Regulation on simplification measures for SMEs including the record-keeping obligation

JULY

Helsinki statement



1. The EDPB Secretariat



Isabelle VEREECKEN
Head of the EDPB Secretariat

Interview with the Head of the EDPB Secretariat, Isabelle Vereecken

2025 has undoubtedly been a year of significant achievements for the EDPB and its Secretariat. In your view, what has been the biggest successes of this year?

Two major successes include the [Helsinki Statement on enhanced clarity, support and engagement](#) and our work clarifying the interplay between the GDPR and digital legislations.

The Helsinki Statement outlines new initiatives to make GDPR compliance easier, strengthen consistency and boost cross-regulatory cooperation. The EDPB has implemented numerous internal measures to ensure these commitments are delivered effectively.

In addition, the EDPB decided to strengthen our dialogue with stakeholders. In November 2025, for example, we consulted stakeholders to identify which templates would be most helpful

to facilitate GDPR compliance. In addition, in December 2025, we held an online stakeholder event on anonymisation and pseudonymisation.

Another important achievement is the interplay guidance, which clarifies the relationship between the GDPR and digital laws. In October 2025, we endorsed [Joint Guidelines with the European Commission on the interplay between the Digital Markets Act \(DMA\) and the GDPR](#). This was the first time the EDPB and the Commission worked on joint guidance.

In addition, the EDPB has adopted [Guidelines on the interplay between the Digital Services Act \(DSA\) and the GDPR](#) and we have worked with the Commission on Joint Guidelines on the interplay between the AI Act and EU data protection laws.

These efforts help ensure legal certainty, strengthen consistency as well as the protection of individuals' fundamental rights in the digital space.

Lastly, I would also like to add: the new EDPB visual identity and the work to prepare the website (to be launched in 2026), for a more user-friendly experience, improved accessibility and easier content search. This project is a great example of cross-team cooperation within the Secretariat, bringing together communications, IT, admin and legal experts.

One of the EDPB's strategic objectives is to strengthen global dialogue and raise data protection standards not only in Europe but worldwide. How has the work of the Secretariat contributed to this goal in the past year?

In 2025, the EDPB advanced its global dialogue by hosting and organising the second meeting with the countries and the organisation with an EU adequacy decision. The Secretariat fostered close cooperation and exchange of information among EDPB members and third countries' DPAs, providing strong organisational support.



The EDPB Secretariat's staff also serve as a unified voice for European Data Protection Authorities (DPAs) in international discussions. In 2025, for example, we took part in the G7 Data Protection and Privacy Authorities roundtable and the Global Privacy Assembly.

In addition, we hosted in our offices in Brussels Data Protection Authorities from Japan, South Korea, Kenya, Brazil but also from the Western Balkans and Eastern Partnership to exchange on our priorities and strengthen collaboration. The EDPB Chair and Secretariat representatives have also participated in global events as speakers and panelists, promoting European data protection standards on the international stage.

The trend toward simplifying GDPR compliance is gaining momentum. As someone who has seen the regulation from its early days, how do you view this push for simplification from a personal point view?

From my experience since the GDPR's early days, the compliance effort was most intense during the GDPR's early implementation and in the years immediately following. European DPAs also had to adapt to this new legal framework, which gave them additional tasks and powers. In Helsinki, the EDPB took a more proactive

approach to support compliance efforts by deciding to develop practical templates to help organisations meet GDPR requirements.

As the digital regulatory landscape evolved and became more complex, the EDPB decided to be part of the solution by working on the interplay guidelines.

I believe that the debate about simplification is healthy and helps maintain relevance and effectiveness in an increasingly interconnected world where data protection laws intersect with other digital regulations. While simplification is necessary, it must be balanced. Effective regulation requires pragmatic adjustments without compromising fundamental rights, particularly privacy and data protection. We support measures that reduce administrative burdens for organisations, as long as they do not weaken the protection of individuals' fundamental rights.

If you could speak to Isabelle in 2018, when the EDPB Secretariat was first established, what would you tell yourself about its growth and great achievements over the years and its increasingly central role in data protection?

My advice to the Isabelle of 2018 would be to start bigger, in particular with staff budget requests. Initially, I took a cautious approach, but given the

continuous growth of our workload, our current staffing levels no longer match our real needs. That said, I am grateful for the 2026 staff increase, which was secured despite tight budget constraints.

I would also tell her that the EDPB will demonstrate its ability to have a central role in data protection, not only in Europe but also globally. Our expertise goes beyond pure data protection as we have an active role in the regulation of the digital society. This is a clear sign of how vital our work has become in European data protection.

Lastly, I would tell her that she will be surrounded by a wonderful and extremely efficient team. I am incredibly proud of what we have achieved, and it is all thanks to a dedicated team that never stops learning, adapting, and pushing forward. The road ahead might be challenging sometimes, but that is what makes it exciting and rewarding. With the same dedication and teamwork, we are prepared to take on new challenges and achieve even bigger milestones to keep making a real impact.

1.1 Mission And Activities

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

The terms of cooperation between the EDPB and the EDPS are established by a [Memorandum of Understanding](#). The EDPS employs the staff at the EDPB Secretariat. However, they work exclusively under the instructions of the Chair of the EDPB. A dedicated title exists in the EDPS budget to cover both the budget of the EDPB Secretariat and of the EDPB as a whole (e.g. meeting costs, translation and interpretation costs). In 2025, it includes 47 staff members who work within the EDPB Secretariat or within the EDPS for the support provided to the EDPB via horizontal administrative services.



Ian Deguara,
Information and Data Protection
Commissioner of Malta

The European Data Protection Board is a strong and unified team of Data Protection Authorities, speaking with one voice. In the digital age, the protection of personal data, especially in the context of artificial intelligence, requires not only responsiveness to emerging challenges, but a shared commitment to responsibility, coherence, and consistency.

The EDPB Secretariat provides analytical and legislative support to the Board. As such, in 2025, the EDPB Secretariat led the drafting of 21 opinions and contributed to a further 8 opinions. The EDPB Secretariat also supports the EDPB in enforcing data protection laws, ensures consistent enforcement and promotes cooperation amongst DPAs.

In addition, the EDPB Secretariat provides the Secretariat of the [Coordinated Supervision Committee \(CSC\)](#). The CSC ensures the coordinated supervision of large scale IT systems and of EU bodies, offices and agencies, in accordance with Art. 62 of Regulation (EU) 2018/1725 or with the EU legal act establishing the large scale IT system or the EU body, office or agency.

The EDPB budget forms part of the broader budget of the EDPS. In 2025, the adopted budget of the EDPB amounted to € 8.823 million. This budget supports the growth of enforcement and litigation activities and covers expenditure for EDPB meetings at the plenary and subgroup level, translation and interpretation costs, IT services, and remuneration of the EDPB Secretariat staff. In 2025, the EDPB Secretariat organised over 500 meetings continuing the trend that started in 2024.

In 2025, the EDPB was involved as a party in 15 cases before the CJEU, one of which was submitted in 2022¹, ten in 2023², two in 2024³, and two in 2025⁴. In addition, in 2025 the EDPB was involved as intervener in one case, in support of the European Data Protection Supervisor

1. Case T-682/22 Meta Platforms Ireland v EDPB.
2. Cases T-183/23 Ballmann v EDPB; Joined cases T-70/23, T-84/23, 111/23 Data Protection Commission v EDPB; T-128/23 Meta Platforms Ireland v EDPB; T-129/23 Meta Platforms Ireland v EDPB; T-153/23 WhatsApp Ireland v EDPB; T-325/23 Meta Platforms Ireland v EDPB; T-1030/23 Tiktok Technology v EDPB; and C-97/23 P WhatsApp Ireland v EDPB.
3. Case T-8/24 Meta Platforms Ireland v EDPB; and Case T-319/24 Meta Platforms Ireland v EDPB.
4. Case C-454/25 P Meta Platforms Ireland v EDPB; and Case C-627/25 P Commission v Ballmann.

(EDPS)⁵. 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.

In the course of 2025, the EDPB has intensified its efforts to make GDPR information more accessible to a wider, non-technical audience by presenting it in clear, straightforward language. This aligns with the Board's objective of simplifying GDPR compliance for organisations, as set out in the EDPB's 2024-2027 strategy and the Helsinki Statement on enhanced clarity, support, and engagement.



Maria Christofides,
Commissioner for Personal
Data Protection, Cyprus

Trust is the currency of the digital era. Data protection is ultimately about building and preserving that trust through consistency, cooperation and respect for personal data protection. The EDPB plays a pivotal role in fostering coherence, legal certainty and constructive dialogue across Europe, ensuring that innovation and fundamental rights advance hand in hand. Through collective actions, the EDPB transforms legal principles into lived reality, reflecting the shared responsibility that underpins the strength of the European data protection framework.

Moving forward in this direction, the Board launched a new outreach project consisting of a series of summaries of EDPB guidelines. The main objective of this project is to help non-expert individuals and organisations identify, in an easier way, the most important points to consider in such EDPB documents. Following the initial summary on the [Guidelines 1/2024 on processing of personal data based on Article 6\(1\)\(f\) GDPR](#) at the end of 2024, the EDPB published five additional summaries in 2025, covering: [pseudonymisation](#), [personal data breaches](#), [blockchain technologies](#), [right of access](#) and the [interplay between the Digital Services Act \(DSA\) and the GDPR](#).

5. Case C-413/23 P EDPS v Single Resolution Board.





Data Protection And Transparency

The EDPB Secretariat is 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 EDPB's operations by facilitating public access to its documents. Initial requests are handled and signed by one of the Deputy Chairs. Confirmatory requests are handled and signed by the Chair. In 2025, the EDPB received 20 requests. Confirmatory applications were received in six cases. The EDPB also received five consultation requests from EDPB members on national access to document requests concerning documents originated from the EDPB. No complaint regarding the EDPB confirmatory decisions for an AtD request was brought to the attention of the European Ombudsman in 2025.

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), which is part of the EDPB Secretariat. In 2025, the EDPB received 12 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 the handling of nine data breaches under Arts. 34 and 35 of Regulation (EU) 2018/1725, one of which required a notification to the EDPS.

IT systems

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

In 2025, the Secretariat successfully addressed over 800 support requests concerning the IMI system and efficiently handled over 10.000 inquiries across all EDPB IT systems (up from 4.200 in 2024), delivering prompt and effective assistance to stakeholders.



Collaborating with the Support Pool of Experts, the EDPB Secretariat introduced a sophisticated statistical application, automating the generation of GDPR activity reports within the IMI. This innovation allows for instant creation of comprehensive reports and figures, eliminating the previously manual and complex processes.

The EDPB HUB maintained its pivotal role as the premier platform for internal communication and information dissemination in 2025. With over 10.000 content pieces created and shared, the platform saw a substantial increase in activity compared to past years. This surge in engagement underscores the HUB's continued importance in facilitating collaboration and knowledge exchange. Additionally, the Secretariat ensured the operation of the EDPB website, which attracted 317.187 visits and recorded 1.516.687 page views throughout the year. Popular sections included "Members, Guidelines, Recommendations, Best Practices, News, Documents, and Opinions". These digital platforms remain essential for advancing the EDPB's mission and boosting operational efficiency.



Isabelle VEREECKEN
Head of the EDPB Secretariat



Gwendal LE GRAND
Deputy Head of
the EDPB secretariat

THE EDPB SECRETARIAT

**Effrosyni
PANAGO**
Administrative
Matters
Sector

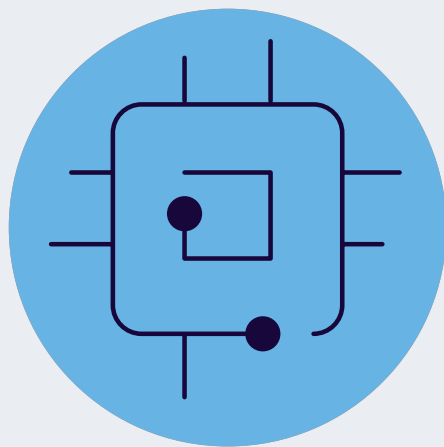
**Ahmed
IMMOUN**
IT Matters
Sector

**Greet
GYSEN**
Information and
Communications
Sector

**Carolina
FOGLIA**
Legal Affairs -
Cooperation and
Enforcement
Sector

**Myriam
GUFFLET**
Litigation and
International
Affairs Sector

2. European Data Protection Board – Activities in 2025



2.1 Bridging Fundamental Rights and Digital Innovation Through GDPR Compliance

Rapid technological developments, particularly the widespread deployment of artificial intelligence, are reshaping how services are designed and delivered. This has led to challenges for regulators, requiring quick adaptation and close cooperation across policy fields.



Zuzana Valková,
President of the Office for
Personal Data Protection
of the Slovak Republic

In 2025, cooperation within the EDPB delivered progress in harmonization, consistency, and legal certainty, alongside initiatives to facilitate GDPR compliance for smaller organisations. In parallel, emerging technologies such as AI posed challenges for safeguarding fundamental rights. Looking ahead, the priority is to shift the AI debate from fascination to responsibility and ensure clear and transparent rules for systems using personal data.

At the same time, the growing complexity of the regulatory landscape has reinforced the need for simplification. More streamlined requirements can help to reduce administrative burdens. In addition, simplification enables organisations to better understand and meet their obligations, which can support compliance.

Alongside these developments, there is increasing public awareness and debate around the need to protect children online. As digital services and AI-driven systems become omnipresent, ensuring that children's rights and well-being are safeguarded

has become a shared priority worldwide. In 2025, Australia was the first country in the world to set a minimum age (under 16) for the use of some social media platforms and oblige them to restrict access to their services. In Europe, the aim is to protect children effectively while avoiding generalised identification or surveillance. In this context, the [EDPB statement on age assurance](#) plays an important role in providing practical guidance and promoting a consistent approach.

2.1.1 Helsinki high-level meeting: enhanced clarity, support and engagement

At a two-day [high-level meeting in Helsinki](#) on 1–2 July 2025, the EDPB agreed on new initiatives to make GDPR compliance easier, strengthen consistency, enhance stakeholder dialogue and reinforce cross-regulatory cooperation in the evolving digital landscape.



Jelena Virant Burnik,
Deputy Chair of the EDPB
and Slovenian Information
Commissioner

The EDPB plays a leading role in ensuring a coherent European data protection framework, by guiding DPAs towards aligned application of the GDPR. In 2025, key achievements included the Helsinki meeting outcomes, the guidelines on legitimate interest and on the DSA-GDPR interplay, and high-level exchanges on cross-regulatory cooperation and AI. The EDPB is an increasingly important catalyst for positive change, and as Deputy Chair, I am honoured to support its mission.

These initiatives aim in particular to support micro, small and medium organisations, enable responsible innovation, and strengthen Europe's competitiveness.

The EDPB reaffirmed the central role of data protection in upholding European values, protecting fundamental rights, and supporting the human-centric use of personal data.

It committed to earlier and more proactive engagement with stakeholders, including public reporting on consultation outcomes.

The EDPB also committed to provide clearer, more practical and accessible guidance, and update its working methods accordingly.

New tools will include harmonised templates, practical resources such as checklists and Frequently Asked Questions (FAQ), and a common data breach notification template.

The EDPB will also enhance consistency in GDPR application and enforcement and deepen cooperation with other regulators to ensure coherent safeguards across the EU’s cross-regulatory framework.



Des Hogan,
Commissioner for Data Protection and Chairperson of the Irish Data Protection Commission, Ireland

In 2025, we reaffirmed our commitment to data protection as a cornerstone of fundamental rights, guided by the Helsinki Statement on enhanced clarity, support and engagement. We deepened cooperation with our EU colleagues, enabling initiatives such as our “Pause Before You Post” public awareness campaign in collaboration with the CNIL, as well as the secondment of staff from peer authorities to the DPC. The DPC would like to thank all our EDPB colleagues for their collaboration and support.

Six months of progress since the Helsinki Statement



Progress since July 2025

GDPR made easy

December 2025 Creation of internal guidance and best practices to ensure EDPB guidance is timely, concise, easy to understand, and practical.

Greater consistency & enforcement

Strengthened stakeholder dialogue

December 2025 Stakeholder event on anonymisation and pseudonymisation.

Cross-regulatory cooperation

October 2025 Joint guidelines by the EDPB and the European Commission on the interplay between Digital Markets Act (DMA) and GDPR.

In the pipeline for 2026

Early 2026 Data Protection Impact Assessment (DPIA) template.

2026 Data breach notification template.

Early 2026 Forms on the EDPB website to signal inconsistencies between national and EDPB guidance.

March 2026 Workshop on complaint handling among Data Protection Authorities (DPAs).

Early 2026 Report on public consultation on blockchain guidelines.

Early 2026 Report on stakeholder event on anonymisation and pseudonymisation.

Throughout 2026 Joint guidelines by the EDPB and the European Commission on the interplay between AI Act and GDPR. More stakeholder and public events.

Summer 2026 Template for cross-regulatory cooperation agreements.

2.1.2 Regulation on procedural rules and Omnibus regulation on the record of processing

The work of the legislator to optimise the application of the digital rulebook continued in 2025. The Regulation 2025/2518 laying down additional procedural rules on the enforcement of GDPR, which was adopted on 26 November 2025, aims to harmonise and streamline cross-border GDPR enforcement. The Digital Omnibus in its turn seeks to simplify regulatory requirements.

Building on the [Vienna Statement](#), the wish list [Letter to the EU Commission on procedural aspects](#), the [EDPB-EDPS Joint Opinion 01/2023](#) and [EDPB Statement 4/2024 on additional procedural rules](#), the EDPB reaffirmed its commitment to improve GDPR enforcement. In line with its [2024-2027 Strategy](#), the EDPB started preparing for the practical implementation of the procedural regulation. In particular, the regulation harmonises some aspects of the enforcement procedure and introduces new legal definitions, steps and deadlines.



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

Ensuring consistent enforcement and legal certainty for individuals and organisations, while keeping data protection at the core, was a key challenge throughout 2025. In next years, the EDPB will become an even more strategic actor at the intersection of data protection, AI, digital markets and innovation policy. Its role will extend to developing practical methodologies, and to safeguarding the autonomy of data protection law within broader regulatory reforms. The EDPB will be central to ensuring that regulatory simplification does not come at the expense of fundamental rights.

After conducting a review of its working methods and procedures, the EDPB adopted a practical implementation plan on 4 November 2025. This initiative aims at ensuring that the DPAs will be ready when the regulation becomes applicable on 2 April 2027. To maximise transparency and ensure clarity with regard to the relevant EDPB guidance, the new EDPB documents will be added to the EDPB website, alongside the existing ones. The EDPB is preparing



the next steps and evaluating whether complementary actions are needed to ease the work of the DPAs.

In November 2025, the European Commission launched its proposal for a Digital Omnibus. The [EDPB-EDPS joint opinion](#), which was adopted in early 2026, strongly urged the co-legislators not to adopt the proposed changes to the definition of personal data as they go far beyond a targeted or technical amendment of the GDPR, they do not accurately reflect the CJEU jurisprudence, and they would result in significantly narrowing the concept of personal data. The opinion also supports several elements of the proposal, such as the increase of the threshold of risk leading to the obligation to notify a data breach, the extension of the deadline to submit such a notification, the proposed common templates and the lists for data breaches and data protection impact assessments.

2.1.3 Cross regulatory cooperation

The EDPB's role in explaining how data protection rules interact with other digital laws became increasingly important in 2025.



Koen Gorissen,
Chairman of the Belgian
Data Protection Authority

The interplay between the various digital regulations is a key common challenge for Data Protection Authorities. In 2025, the EDPB played a crucial role in helping authorities address this regulatory complexity. The Belgian DPA is specifically pleased to support the EDPB's important work in the field of cross-regulatory cooperation agreements.

2.1.3.1 DSA - GDPR Guidelines

The EDPB adopted [Guidelines 3/2025 on the interplay between the Digital Services Act \(DSA\) and the GDPR](#) on 11 September 2025, and submitted them to a written public consultation (see Chapter 2.2 for further details).



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

The year 2025 was intense and full of challenges. Growing activities and increasingly complex issues pushed us to find more efficient ways to protect the right to personal data. The implementation of artificial intelligence and other EU digital agenda legislation requires a fresh approach from DPAs, especially in interaction with the GDPR. In this context, the Helsinki Statement adopted in July 2025 is a key step, addressing today's challenges and demonstrating the EDPB's commitment to consistent data protection.

2.1.3.2 DMA - GDPR Guidelines

In October 2025, the EDPB and the European Commission endorsed draft [Joint Guidelines on the interplay between the Digital Markets Act \(DMA\) and the GDPR](#) (see Chapter 2.2 for further details).

The preparation of these guidelines demonstrates enhanced cooperation between the EDPB and the Commission. By contributing to a coherent framework for gatekeepers' obligations, the EDPB supported the development of consistent enforcement mechanisms across regulatory domains and helped foster a predictable compliance environment for digital services operating in the EU.

2.1.3.3 Position Paper on interplay between data protection and competition law

In January 2025, the EDPB adopted a [Position Paper on the interplay between data protection and competition law](#). The paper highlights how data-driven business models can raise issues under both frameworks and identifies situations where closer cooperation between data protection and competition authorities could be beneficial. It points to shared areas of interest such as data concentration, access to large datasets, and the ways in which market power can influence individuals' ability to exercise their rights under data protection law.

The position paper also calls for more structured exchanges between authorities and clearer communication to ensure that measures taken under one framework do not weaken protections under the other. This work builds on the EDPB's broader engagement with other regulators, including recent cooperation with the Commission, competition and consumer authorities on "consent or pay" models, and joint work with the EU AI Office on the Opinion concerning AI models.

2.1.4 The EDPB in a global context

One of the EDPB's strategic objectives is to engage with the international community to promote a high level of data protection and to ensure effective protection of personal data beyond EU borders. To this end, the EDPB continued to intensify its international engagement throughout 2025, both through high-level speaking engagements by the Chair and active participation in key global fora such as among others, the Global Privacy Assembly (GPA), the Spring Conference and the G7 DPA Roundtable.

In June, the EDPB Chair took part in the G7 DPA Roundtable in Ottawa, engaging with Data Protection Authorities (DPAs) of the G7 members in strategic discussions aimed at harmonising global data protection policies and addressing the challenges posed by new technologies.

At the 47th GPA in Seoul in September, the Chair participated in high-level sessions and engaged with GPA members on strategic topics for data protection, speaking on a panel on **Lawfulness of Processing Personal Data for Purposes of AI** and delivering the closing remarks.

Altogether, the EDPB Chair participated in 27 speaking engagements in 2025, while Deputy Chairs contributed to four additional events.

2.1.4.1 EDPB initiative with countries with an EU adequacy decision and Taskforce on International Engagement

Complementing these engagements, the EDPB continued its work in the context of other international meetings and task forces, including regular interactions with third-country authorities under the adequacy framework and ongoing contributions to the Task Force on International Engagement which the Board launched to streamline its global outreach efforts.

The taskforce met several times during the year to strengthen exchanges between

EDPB members as regards the participation in multilateral fora in the field of data protection and privacy (for instance, Council of Europe, Global Privacy Assembly, OECD, etc.)

In December 2025, the EDPB organised the [second meeting of the EDPB initiative with DPAs from countries with an EU adequacy decision](#). During the meeting, the group discussed how to foster cooperation on advisory work and guidelines, as well as on enforcement activities.



2.2 Ensuring Consistent Protection



Jekaterina Macuka,
Director of the Data State
Inspectorate of Latvia

Effective data protection is not only about individual cases, but about solutions that protect many people at once. As an independent guardian of fundamental rights, the EDPB brings authorities together to find a balanced “golden middle” - ensuring that data protection is not seen as an obstacle to technology, but as a foundation for trust, responsible innovation and a shared European digital future.

2.2.1 Guidance and Recommendations

One of the EDPB’s core competences is to clarify the GDPR by issuing guidance. Since 2018, the EDPB established a well-defined and comprehensive [repository of guidelines and recommendations](#). This ensures that DPAs apply data protection laws consistently and it further strengthens stakeholder compliance. The EDPB continues to build and expand its guidance and makes a consistent effort to incorporate stakeholder input, which is collected via public consultation.

In 2025, the EDPB adopted three new guidelines, as well as one guideline following public consultation, and two set of recommendations. In addition, the EDPB and the Commission endorsed one set of joint guidelines (see Annexes, Section 4.1 for the complete list of guidelines and recommendations).

2.2.1.1 Guidelines 1/2025 on Pseudonymisation

On 16 January 2025, the EDPB adopted [Guidelines on Pseudonymisation](#). These guidelines explain

the definition and the role of pseudonymisation, as a safeguard that may be appropriate and effective to meet data protection obligations. More specifically, the guidelines explain that pseudonymisation can help organisations meet their obligations relating to the implementation of data protection principles, data protection by design and default, and security. The guidelines analyse technical measures and safeguards, when using pseudonymisation, to ensure confidentiality and prevent unauthorised identification of individuals. These guidelines were submitted to a written public consultation, and they are complemented by [a summary](#). Moreover, the EDPB organised a stakeholder event on this topic on 12 December 2025 (more information in Section 2.2.5.3).

2.2.1.2 Guidelines 02/2025 on processing of personal data through blockchain technologies

The EDPB adopted [these guidelines](#) on 8 April 2025 and submitted them for a written public consultation, on the basis of which the final version will be produced. A blockchain is a distributed digital ledger system that can confirm transactions and establish who owned a digital asset (such as cryptocurrency) at a given time. Blockchains can also support the secure handling and transfer of data, ensuring its integrity and traceability.

As the use of blockchain technologies is expanding, the EDPB guidelines are addressed to organisations who plan to make use of blockchain technologies. They outline the key elements to consider to ensure compliance with several provisions of the GDPR. They assess the different possible architectures and their implications for the processing of personal data.

The guidelines highlight the importance of implementing technical and organisational measures at the earliest stages of the design of the processing. They clarify the roles and responsibilities of the different actors in a blockchain. The guidelines

provide examples of different techniques for data minimisation, as well as for handling and storing personal data. As a general rule, storing personal data in a blockchain should be avoided if this conflicts with data protection principles.

Finally, the Board highlights key elements on guaranteeing the rights granted to individuals by the GDPR in the context of blockchain technologies, especially transparency, rectification and erasure of personal data. A summary on these guidelines is also [available here](#).

2.2.1.3 Guidelines 3/2025 on the interplay between the DSA and the GDPR

The EDPB adopted [these guidelines](#) on 11 September 2025 and submitted them for public consultation, following which a final version will be produced. These guidelines are the first adopted by the EDPB addressing the interaction between the GDPR and the EU's digital legislation. They aim to ensure a consistent and coherent interpretation and application of the Digital Services Act (DSA) and the GDPR where DSA obligations involve the processing of personal data by online intermediary service providers, including online platforms and search engines.

The guidelines analyse the interplay with the GDPR of certain provisions of the DSA concerning the processing of personal data by intermediary service providers. In particular, the guidelines clarify how GDPR principles, concepts and safeguards apply in the context of DSA provisions relating to notice-and-action mechanisms for reporting illegal content, recommender systems, transparency of advertising, deceptive design patterns and measures to ensure a high level of privacy, safety and security for minors, including the prohibition of profile-based advertising directed at them. They also address the prohibition of profiling-based advertising using special categories of personal data. In addition, the guidelines also underline the importance of cooperation and mutual consultation between Digital Services Coordinators, the European Commission and DPAs, with a view to enhancing coordinated enforcement, legal certainty for service providers, and the effective protection of individuals' fundamental rights and freedoms. An EDPB factsheet summarising these guidelines is [available here](#).

2.2.1.4 Guidelines 02/2024 on Article 48 GDPR

Following public consultation, the EDPB adopted on 4 June 2025 the final version of [Guidelines](#)

[02/2024](#) on data transfers to third country authorities. In its guidelines, the EDPB zooms in on Art. 48 GDPR and clarifies how organisations can best assess under which conditions they can lawfully respond to requests for a transfer of personal data from third country authorities (i.e. authorities from non-European countries).

The EDPB explained that judgements or decisions from third country authorities cannot automatically be recognised or enforced in Europe. As a general rule, an international agreement may provide for both a legal basis and a ground for transfer. In exceptional circumstances, other legal bases or other grounds for transfer could be considered on a case-by-case basis.

The modifications introduced in the updated guidelines aim to provide further clarifications on elements brought up during the consultation. For example, the updated guidelines address the situation where the recipient of a request is a processor. They also address the situation where a subsidiary in Europe is asked to answer a request received by the mother company in a third country from that third country authority.

2.2.1.5 Joint guidelines on the interplay between the Digital Markets Act (DMA) and the GDPR

The EDPB and the European Commission endorsed [these joint guidelines](#) on 9 October 2025 and submitted them for public consultation, after which a final version will be produced. These are the first guidelines jointly prepared by the EDPB and the Commission and are intended to facilitate a coherent and consistent application of the DMA and the GDPR, in line with the [EDPB's 2024-2027 Strategy](#) and the objectives of the [Helsinki Statement](#). The guidelines aim to increase legal certainty for gatekeepers, business users, beneficiaries and individuals, while simplifying compliance with EU digital and data protection rules.

The guidelines clarify how GDPR principles, concepts and safeguards apply in the context of DMA obligations that entail the processing of personal data by gatekeepers. In particular, they explain how gatekeepers can implement DMA provisions that explicitly refer to GDPR concepts, such as the requirements for specific choice and valid consent under Art. 5(2) DMA, in order to lawfully combine or cross-use personal data across core platform services. The guidance also addresses other relevant DMA obligations, including those related to the distribution of third-party apps

and app stores, data portability, access to data, and the interoperability of messaging services.

The guidelines also emphasise the complementary objectives of the DMA and the GDPR in the digital environment, with the GDPR focusing on the protection of individuals' rights and personal data, and the DMA aiming to ensure fairness and contestability in digital markets.

By clarifying common touchpoints between the two legal frameworks, the joint guidance supports a consistent, effective and complementary application of EU digital and data protection law.

The guidelines were subject to a joint public consultation, which closed on 4 December 2025, providing stakeholders with the opportunity to submit comments and feedback. The final text, incorporating input received during the consultation, will be prepared jointly by the EDPB and the European Commission and adopted by both institutions.

2.2.1.6 Interplay GDPR – AI Act

Further joint work is ongoing with the European Commission, including with the AI Office, on guidelines addressing the interplay between the AI Act and EU data protection laws, with the aim of maintaining coherent and consistent safeguards for the protection of personal data.

2.2.1.7 Recommendations 1/2025 on the 2027 WADA World Anti-Doping Code

On 11 February 2025, upon request from the European Commission, the EDPB adopted its [Recommendations on the 2027 WADA World Anti-Doping Code](#), assessing the compatibility of the Code and its complementing International Standard for Data Protection (ISDP) with the GDPR. The EDPB underlined the need for Member States to ensure that national anti-doping measures, adopted in order to transpose the Code, are in line with the GDPR.

The EDPB welcomed certain positive changes brought since its previous letter of 2019, but raised concerns about some other elements, mainly concerning consent, purpose limitation, and attribution of roles.

2.2.1.8 Recommendations 2/2025 on the legal basis for requiring user account creation on e-commerce websites

On 4 December 2025, the EDPB adopted [Recommendations on the legal basis for requiring the creation of user accounts on](#)

[e-commerce websites](#), and submitted them to public consultation. These recommendations aim to clarify under which conditions e-commerce websites may require users to create an account.

The EDPB underlined that, as a general rule, users should be able to make purchases on e-commerce websites without being required to create an account. In this regard, the Board recommended that e-commerce websites offer alternatives such as a “guest” mode or the voluntary creation of an account, in line with the principles of data protection by design and by default and with the objective of minimising the processing of personal data. At the same time, the EDPB acknowledged that mandatory account creation may be justified in a limited number of situations, for example in the context of subscription-based services or access to exclusive offers.

Overall, the recommendations reflect the EDPB's commitment to promoting pragmatic, user-friendly and privacy-protective practices in the e-commerce sector.

2.2.2 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.

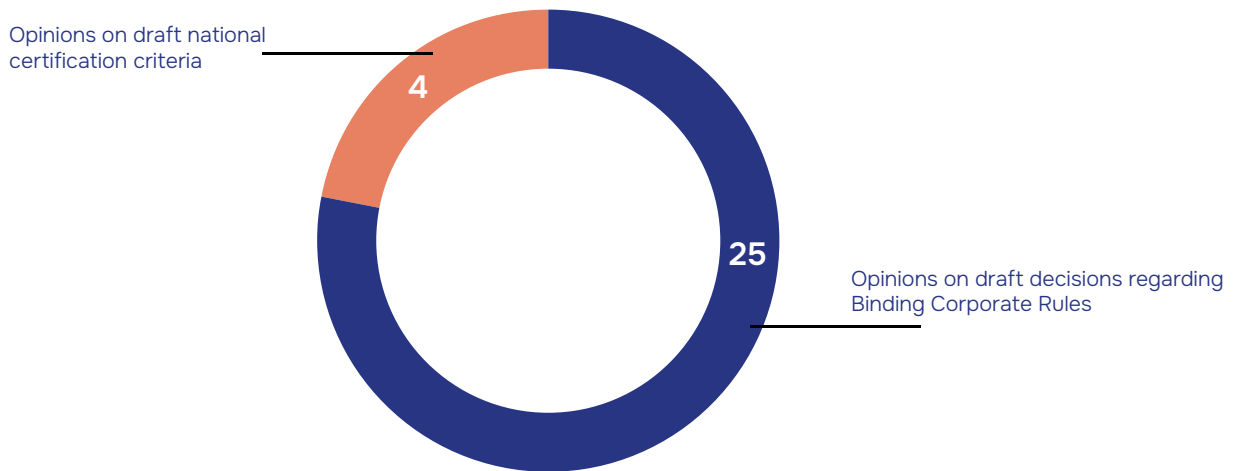
DPAs may also request a consistency opinion from the EDPB when considering measures that could impact multiple jurisdictions. Once issued, these opinions serve as guiding documents, enabling DPAs to finalise their decisions while ensuring alignment with the GDPR standards. In 2025, 29 opinions were issued under Art. 64(1) GDPR.

2.2.2.1 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 and not requiring Data Protection Impact Assessments

Consistency opinions in 2025



(DPIAs): these lists identify activities that are likely to pose significant risks to individuals' rights and freedoms, and kinds of processing operations for which no DPIA is required;

- ▶ 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 2025, the EDPB adopted 29 Art. 64(1) GDPR opinions, reflecting its continued commitment to promoting harmonisation. Since its establishment in 2018, the EDPB has issued a total of 217 Art. 64(1) opinions, demonstrating the sustained importance of this mechanism in supporting a harmonised application of the GDPR. (See Annexes, Section 4.2 for the complete list of opinions adopted in 2025).

2.2.3 Legislative Consultation

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

Adequacy decisions, which are negotiated by the European Commission, are a key instrument of the GDPR for data transfers and require the EDPB's consultation.

In 2025, the EDPB provided 5 opinions on the adequate level of protection of personal data in third countries and in an international organisation.

2.2.3.1 Opinion 06/2025 regarding the extension of the European Commission Implementing Decisions under the GDPR and the LED on the adequate protection of personal data in the United Kingdom

The EDPB opinion addressed the proposed extension of the two UK adequacy decisions (under the GDPR and the LED), which were set to expire on 27 June 2025. The opinion only concerned the proposed 6-month extension of these adequacy decisions and did not address the level of protection of personal data afforded in the UK. The EDPB recognised the need for a technical and time-limited extension up to 27 December 2025, so as to provide the European Commission with sufficient time to evaluate the updated UK legal framework. The EDPB stressed that this extension was exceptional and due to the ongoing legislative developments in the UK.

2.2.3.2 Opinion 07/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the European Patent Organisation (EPO)

The Board adopted an [opinion on the Commission's draft adequacy decision regarding EPO](#). The Board positively noted that the EPO data protection framework is largely aligned with the EU data protection framework, including on data protection rights and principles. This was the first draft adequacy decision concerning an international organisation (and not a country). The successful adoption of the adequacy decision shows that the GDPR and, in particular, its transfer provisions, can facilitate safe data flows from Europe to international organisations, while taking into account their status.

2.2.3.3 Opinion 26/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom

This [EDPB opinion](#) addressed the Commission's draft adequacy decision on the extension of the validity of the UK adequacy decision under the GDPR until December 2031. The EDPB positively noted the continuing alignment between the UK and EU data protection frameworks. According to the Board, most of the changes introduced to the UK's data protection framework aim to clarify and facilitate compliance with the law. Considering the most recent legislative developments in the UK framework, the EDPB also invited the Commission to make a more detailed assessment on certain points in its decision and to monitor several aspects, such as the rules on transfers from the UK to third countries, the restructuring of the Information Commissioner's Office, the removal of the principle of primacy of EU law in the Retained EU Law Act 2023 or the use by the UK Government of technical capability notices requiring companies to circumvent encryption.

2.2.3.4 Opinion 27/2025 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data by the United Kingdom

This [EDPB opinion](#) addressed the European Commission's draft adequacy decision on the extension of the validity of the UK adequacy decision under the LED until December 2031. While welcoming the continuous alignment between the UK and EU data protection frameworks, the EDPB encouraged

the Commission to complement its assessment on specific aspects of the new legal framework which may affect the level of protection for data subjects, such as the extended national security exemptions, the changes to the rules governing onward transfers of personal data to third countries and the more permissive approach and conferral of new powers to the Secretary of State in relation to automated decision-making. Finally, the EDPB reiterated the need for the Commission to closely monitor the application of corrective powers and of remedies for individuals in the UK data protection framework.

2.2.3.5 Opinion 28/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by Brazil

The EDPB adopted [its opinion on the European Commission's draft adequacy decision on Brazil](#). The EDPB positively noted that the Brazilian data protection framework establishes requirements that are closely aligned with the GDPR and the case law of the Court of Justice of the European Union, in relation, for instance, to the principles, data subject rights, transfers, oversight and redress mechanisms. Moreover, the EDPB invited the Commission to further clarify certain aspects in its decision, as well as to monitor the practical implementation and concrete impact of certain features of the Brazilian framework, such as the limitations on transparency related to commercial and industrial secrecy and the rules on onward transfers.

In relation to access and use by Brazilian public authorities of personal data transferred to controllers and processors in Brazil for criminal law enforcement and national security purposes ('government access'), the EDPB noted that the General Data Protection Law in Brazil (LGPD) does not apply to data processing conducted for the exclusive purposes of public safety, national defence, state security, or the investigation and prosecution of criminal offenses. At the same time, the EDPB positively noted that the Federal Supreme Court of Brazil, in its case-law, has interpreted the LGPD in a way that expanded its partial applicability to the processing of personal data for criminal investigations and maintenance of public order. In light of this, the Board invited the Commission to further assess and clarify, in the draft decision, the applicability of the Brazilian data protection law in case of personal data processing for criminal law enforcement purposes.

2.2.3.6 EDPB-EDPS Joint Opinion 01/2025 on the Proposal for a Regulation on simplification measures for SMEs and SMCs, in particular the record-keeping obligation under Art. 30(5) GDPR

On 8 July 2025, the EDPB and the EDPS adopted [Joint Opinion 01/2025 on the Proposal for a Regulation as regards the extension of certain mitigating measures available for small and medium sized enterprises \('SMEs'\) to small mid-cap enterprises \('SMCs'\) and further simplification measures](#). Following the adoption of this Proposal on 21 May 2025, the Commission formally consulted the EDPB and the EDPS in accordance with Art. 42(2) of Regulation (EU) 2018/1725.

The Proposal aimed at modifying the derogation under Art. 30(5) GDPR by providing that the record-keeping obligation would not apply to an enterprise or organisation employing fewer than 750 persons unless the processing they carry out would likely to result in a high risk to data subjects' rights and freedoms. In addition, the Proposal introduced a definition of SMEs and SMCs in Art. 4 GDPR and extended the scope of Arts. 40(1) and 42(1) GDPR to the SMCs.

The joint opinion supported the general objective of the Proposal to reduce the administrative burden for SMEs and SMCs as long as pursuing this objective does not result in lowering the protection of the fundamental right to protection of personal data. In this regard, it welcomed that the proposed modifications to the GDPR were targeted and limited in nature and did not affect the core principles and other obligations under the GDPR.

The EDPB and the EDPS welcomed the clarification and simplification efforts concerning the conditions in which the derogation under Art. 30(5) GDPR would apply by providing that this derogation would not apply to processing 'likely to result in a high risk'. In this regard, they highlighted that the processing of personal data covered under Arts. 9 and 10 GDPR is important to assess whether the processing is likely to result in a high risk. They suggested some improvements to the Proposal.

The EDPB and the EDPS noted that enterprises and organisations exempted from keeping a record of processing activities would have the flexibility to choose the most appropriate methods to ensure and demonstrate compliance. However, they would also need to ensure that those methods adequately support compliance with the GDPR and do not negatively impact the rights of data subjects.

2.2.4 Stakeholder Consultation

2.2.4.1 Public consultation

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

In 2025, 5 public consultations were launched on [Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation, Guidelines 3/2025 on the interplay between the DSA and the GDPR, Guidelines 02/2025 on processing of personal data through blockchain technologies, Guidelines 01/2025 on Pseudonymisation and Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites](#).

In addition, following the [Helsinki Statement on enhanced clarity, support and engagement](#), the EDPB intends to develop a series of ready-to-use templates for organisations. Therefore, the EDPB organised a [public consultation to understand which templates organisations consider would be most useful for them](#) (e.g. privacy notice template, record of processing activities template, etc.). The public consultation started on 5 November 2025 and ended on 3 December 2025.

2.2.4.2 Survey on Practical Application of Adopted Guidance

Under Art. 71(2) GDPR, the EDPB conducted its eighth annual survey to gather feedback on the effectiveness, clarity, and accessibility of the EDPB's guidance issued in 2025. In previous years, the survey targeted key stakeholders, including academics, legal professionals, business and industry representatives, and non-governmental organisations.

For the first time, this annual survey was addressed to Data Protection Authorities (DPAs), ensuring that a comprehensive range of European perspectives was captured. A total of 18 DPAs responded.

The survey explored how DPAs publish EDPB guidelines, whether directly for national use or through national adaptations, as well as which recently issued guidelines and opinions were translated into their national languages in 2025. The survey also examined the channels used to make these materials available and collected feedback on which aspects of the EDPB's work and documents were found most and least helpful.

While most respondents indicated that their DPA publish the EDPB guidelines directly for national use without modification, several respondents reported complementing this approach by also issuing national guidelines based on the EDPB ones. Only a limited number of DPAs indicated that they rely exclusively on national guidelines derived from the EDPB guidelines.

Overall, the responses reflect a broad engagement by DPAs in making the most recent EDPB guidelines accessible in their languages.

Most respondents reported having translated several EDPB guidelines adopted in 2025 into their national language(s). Others reported focusing primarily on the translation of guidance issued prior to 2025.

Concerning the guidance adopted in 2025, the EDPB [Guidelines 02/2024 on Article 48 GDPR](#) (final versions adopted after public consultation),

the [Guidelines 3/2025 on the interplay between the Digital Services Act \(DSA\) and the GDPR](#), and the [Joint Guidelines by the EDPB and the European Commission on the Interplay between the Digital Markets Act \(DMA\) and the GDPR](#), were the guidelines most frequently cited as having been translated in 2025.

Several DPAs also reported publishing [Guidelines 02/2025 on processing of personal data through blockchain technologies](#) and [Guidelines 01/2025 on Pseudonymisation](#) into their national languages.

Half of the respondents reported using their website as the primary channel to make EDPB guidelines accessible to their audience. Among the other half, most indicated that, in addition to their website, they make use of social media platforms to provide links directing users to the EDPB website.

Data Protection Authorities were also consulted on the publication of the most recent EDPB opinions into their national languages in 2025. Among the documents mentioned by some DPAs are [Opinion 07/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation \(EU\) 2016/679 on the adequate protection of personal data by the European Patent Organisation](#) and [EDPB/EDPS Joint Opinion 01/2025 on the Proposal for a Regulation introducing simplification measures for SMEs and micro-enterprises](#),



in particular the exemption from record keeping obligations under Article 30 (5) GDPR.

DPA's that do not publish translations of the EDPB opinions still take steps to ensure these documents are visible and accessible in various ways. These measures include promoting them through their social media channels with links to the EDPB website, translating EDPB press releases that convey the main messages of the adopted opinion along with a link to the EDPB website, drafting brief summaries with direct links to the corresponding EDPB pages, and including translations of relevant sections to ensure clarity and accessibility for national stakeholders.

All respondents regard the work of the EDPB and its guidance as highly valuable and useful for their activities. DPA's emphasized the usefulness of the EDPB work in ensuring harmonisation, consistency and clarity and reducing fragmented interpretations of the law, particularly by focusing on the interplay between data protection and digital laws.

More specifically, several DPA's referred to the work on pseudonymisation and anonymisation, the interplay between the DSA and the GDPR, and the DMA and the GDPR, the [Recommendations on the legal basis for requiring the creation of user accounts on e-commerce websites](#), and all the projects developed within the framework of the [Support Pool of Experts \(SPE\) programme](#).

The efforts based on the [Helsinki statement on enhanced clarity, support and engagement](#), including making GDPR compliance easier, strengthening dialogue with stakeholders, providing more accessible and ready-to-use guidance (such as templates, checklists, and FAQs), and aligning national and EDPB guidance, was positively received. One respondent also highlighted the creation of summaries to explain the EDPB guidance to non-experts in a clearer way as a positive aspect.

Finally, some respondents shared feedback on aspects that could be further improved to enhance the usefulness of the EDPB work and documents. Suggestions included providing a clearer timeframe for the outcomes of public consultations and the finalisation of documents. The EDPB is already working on the points mentioned, in line with the actions arising from the objectives outlined in the Helsinki statement.

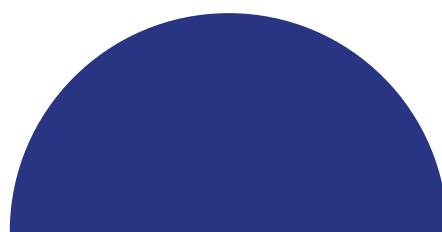
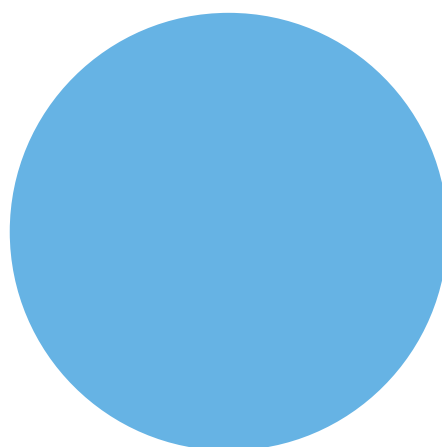
2.2.4.3 Stakeholder Events

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.

In December 2025 the Board organised a [stakeholder event on anonymisation and pseudonymisation](#) aimed at collecting input from stakeholders on implications of the CJEU's ruling of 4 September 2025 in Case C-413/23 P – EDPS v. Single Resolution Board.

Over 100 individuals representing European sector associations, organisations or NGOs and individual companies, law firms or academics took part in the event. In several breakout sessions, they debated a discussion paper listing key questions related to the CJEU's ruling.

As part of its Helsinki commitments, the EDPB will systematically publish reports about the input received during its stakeholder events.



3. Supporting Enforcement



3.1 EDPB Activities To Support GDPR Enforcement And Cooperation Among DPAs

The EDPB kept working to deliver on its commitment to support the DPAs with their enforcement tasks, including by improving the functioning of the cooperation and consistency mechanisms.

In this context, the EDPB dedicated time and resources to develop a practical implementation plan identifying concrete actions to ensure the smooth application of the new Procedural Regulation (see Section 2.1.2 for more details).

3.1.1 Coordinated Enforcement Framework

The importance of consistent enforcement through cooperation has been emphasised by the EDPB ever since the adoption of the GDPR.

In 2020, the EDPB set up a [Coordinated Enforcement Framework \(CEF\)](#), with the aim of streamlining enforcement and cooperation among DPAs, in line with its 2021-2023 Strategy.

The CEF consists of annual joint actions on a specific topic, including activities such as joint information gathering, enforcement sweeps as well as joint investigations. These annual coordinated enforcement efforts are intended to improve compliance, empower individuals to exercise their rights and increase awareness of data protection issues.

In January 2025, the EDPB adopted a [report on the implementation of the right of access by controllers](#). The report summarises the outcome of a series of coordinated national actions carried out in 2024 under the Coordinated Enforcement Framework (CEF). It lists the issues that were observed for some controllers, along with a series of recommendations to help them implement the

right of access. A central element is controllers' awareness of the [EDPB Guidelines 01/2022 on data subjects rights – Right of access](#) and whether these guidelines are followed in practice.

For its [2025 Coordinated Enforcement Action](#), the EDPB selected the implementation of the right to erasure ('right to be forgotten') by controllers, as it is one of the most frequently exercised GDPR rights and one about which DPAs frequently receive complaints from individuals.

Throughout 2025, 32 DPAs across Europe took part in this initiative. A total of 764 controllers across Europe responded to the action, ranging from small and medium-sized enterprises (SMEs) to big companies active in many different industries and fields, as well as various types of public entities.

DPAs checked how controllers handle and respond to the requests for erasure that they receive and, in particular, how they apply the conditions and exceptions for the exercise of this right.

The EDPB report (published in February 2026) analyses some of the most recurring issues observed by DPAs during the year and includes non-binding recommendations for each of them. The EDPB report also maps the extensive guidance documents and templates that exist at national level (both general and targeted to specific context) and more generally, the actions that participating DPAs carried out with respect to the right to erasure.

3.1.2 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.

The EDPB published the deliverables of 7 SPE projects that were launched in 2024. Nine new projects were also launched to enhance GDPR compliance and enforcement across the EU. These SPE projects, which are summarised below, included six new reports, a new version of the website auditing tool (WAT) as well as a video tutorial for the tool.

3.1.2.1 AI: Complex Algorithms and Effective Data Protection Supervision

Project completed by the external expert Dr. Kris SHRISHAK in March 2024 and published by the EDPB in January 2025.

The [AI: Complex Algorithms and Effective Data Protection Supervision](#) project aims at helping Data Protection Authority regarding various aspects related to AI. In particular, it helps clarifying methods and tools for bias evaluation and implementation of data subjects' rights.

3.1.2.2 AI Privacy Risks & Mitigations Large Language Models (LLMs)

Project completed by the external expert Isabel Barbera in April 2025 and published by the EDPB in April 2025.

Large Language Models (LLMs) represent a transformative advancement in artificial intelligence. They are deep learning models designed to process and generate human-like language trained on extensive datasets. Their applications are diverse, ranging from text generation and summarisation to coding assistance, sentiment analysis, and more.



Georgios Batzalexis,
President of the Hellenic DPA

AI is reshaping our digital world, and 2025 proved how essential it is to ground that change in fundamental rights. The EDPB helps steer this transformation toward a future where innovation, trust, and European values advance together.

The [AI Privacy Risks & Mitigations Large Language Models \(LLMs\)](#) report puts forward a comprehensive risk management methodology and practical mitigation measures for common privacy risks

in LLM systems. In addition, the report provides use cases examples on the application of the risk management framework in real-world scenarios:

- ▶ first use case: a virtual assistant (chatbot) for customer queries,
- ▶ second use case: LLM system for monitoring and supporting student progress and,
- ▶ third use case: AI assistant for travel and schedule management.

3.1.2.3 Two Training curricula on AI and data protection: Law & Compliance in AI Security & Data Protection and Fundamentals of Secure AI Systems with Personal Data

Law & Compliance in AI Security & Data Protection project completed by external expert Dr. Marco ALMADA in December 2024 and published by the EDPB in June 2025.

Fundamentals of Secure AI Systems with Personal Data project completed by external expert Dr. Enrico GLERAN in December 2024 and published by the EDPB in June 2025.

The [Law & Compliance in AI Security & Data Protection](#) project is a training for data protection officers (DPOs) addressing the current AI needs and skill gaps. The training provides a comprehensive foundation on legal and compliance issues in AI security and personal data protection. It offers a deeper understanding through practical case studies primarily focused on the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AI Act), the Data Act, and other relevant European regulations.

In addition, the EDPB also launched the [Fundamentals of Secure AI Systems with Personal Data](#) project. The Fundamentals of Secure AI Systems with Personal Data is a training for cybersecurity professionals, developers and deployers of AI systems on AI security & Personal Data Protection which addresses the current AI needs and skill gaps. The training aims at helping these stakeholders to reskill and upskill their technical capacity to design and implement advanced AI-enabled and data-driven systems. It integrates data protection and privacy principles with fundamental AI ethics principles in AI development.

The Board decided to publish both documents as PDF files. Considering the very fast evolution of AI, the EDPB also decided to launch a new innovative initiative consisting of a modifiable community

version of the reports⁶. The EDPB has started working with the authors of both reports to import them in its Git repository to allow, in a near future, any external contributor, with an account on this platform and under the condition of the Creative Commons Attribution-ShareAlike license, to propose changes or add comments to the documents.

3.1.2.4 The Digital Euro and its token-based offline modality

The project was completed by the external expert Prof. Dr.-Ing. Tibor Jager in September 2025 and published by the EDPB in October 2025.

The EDPB has been working to ensure the highest standards of data protection and privacy in the context of the establishment of the digital euro. For example, the EDPB has adopted a [joint opinion](#) with the European Data Protection Supervisor (EDPS) on the [Proposal for a Regulation on the establishment of the digital euro](#).

Decisions regarding the design of the digital euro have significant implications for the rights and freedoms of European individuals as well as for their ability to use data protection-friendly and digital payment methods in the future.

Taking into consideration the joint opinion by the EDPB and the EDPS, the EDPB requested an expert to make an in-depth assessment of the practical feasibility of the “token-based offline modality”, which the EDPB supports. The EDPB also asked the expert to investigate how this solution, suggested by the European Commission and the Eurosystem, can be implemented to ensure the very high level of protection envisaged.

As a result, [this report](#) explores the technical feasibility, inherent limitations, possible approaches, and security considerations related to the development of a cash-like, anonymous, and double-spending resistant offline modality for the digital euro.

3.1.2.5 EDPB website auditing tool

The [EDPB website auditing tool](#) (WAT) helps analyse whether websites are compliant with the law. The software allows the preparation, completion and evaluation of audits directly in the tool by a simple visit to the website concerned.

In 2025, the EDPB had two parallel projects to improve the software and its adoption:

1. A new version of the software

The project was completed and published by the external expert Dr. Jérôme Gorin in September 2025.

Following the success of the version 1 and 2 of the EDPB WAT, a new project was started to create a new version of the EDPB WAT software, facilitating sharing audits and knowledge data bases within an organisation. This project main new feature is thus a new server to share audits and databases among colleagues. This backend has also been made available as Free and Open Source software (under EUPL licence) and can be accessed at <https://code.europa.eu/edpb/edpb-website-auditing-tool-backend>

2. A video tutorial of the website auditing tool

The project was completed by the external expert Mirko Carmia and published in July 2025.

This project concerned the creation of a comprehensive 7 minute animated video tutorial for the EDPB Website Auditing Tool. This video serves as an essential resource for anyone to get acquainted with the software and use it to its full potential.

3.1.2.6 EDPB Bootcamp on AI & AI Auditing

In addition to these initiatives, in October 2025 the EDPB organised its third Bootcamp, which covered the topics of AI and AI Auditing. The event brought together 50 participants from 24 countries, as well as the EDPS, for a series of expert-led sessions, workshops and trainings. PEReN (Pôle d’Expertise de la Régulation Numérique) organised a first workshop focused on SDK analysis while a colleague from the Dutch DPA provided a hands-on workshop dedicated to algorithm creation. Those workshops were complemented by various presentations. This included a presentation of the abovementioned SPE projects providing training curriculum on AI and data protection, as well as presentations by colleagues from the French DPA and EDPS, sharing experience in both a priori and a posteriori audits of AI models and AI based processing activities. The success of the bootcamp demonstrated the importance of

6. Reports available here: <https://law-and-compliance-in-ai-security-and-data-protection-e4e0c8.pages.code.europa.eu/>; <https://fundamentals-of-secure-ai-systems-with-personal-data-9cd9e2.pages.code.europa.eu/>

capacity-building and cross-border collaboration in addressing new data protection challenges.

3.1.3 Taskforces

In 2025, the rapid advancements in artificial intelligence (AI) prompted the EDPB to extend the mandate of the ChatGPT Taskforce in order to cover Generative AI. The scope of the Taskforce on Generative AI Enforcement is to serve as a platform for the exchange of information on investigations related to Generative AI cases in order to enhance cooperation between DPAs and ensure compliance with the GDPR.

The substantive content of these exchanges relates to investigations involving entities without an establishment in Europe. In this context, the Taskforce also aims at facilitating coordination of external communication by DPAs on enforcement activities concerning Artificial Intelligence.

3.2 Litigation

In 2025, the EDPB's role in litigation before the CJEU continued to expand, with the Board acting as a party in 15 cases, a steady accumulation of proceedings submitted since 2022. Most of the cases concerned applications for annulment against binding decisions adopted by the EDPB. The two cases submitted in 2025 were appeals: one in relation to an application for annulment against an urgent binding decision, another in relation to a complainant's right to access the file under Article 41(2)(b) of the EU Charter.

The following table provides an overview of the litigation cases involving the EDPB as a main party⁷, which were still ongoing or closed in 2025:

Case ref.	Subject matter	Status
C-97/23 P	Appeal brought by WhatsApp Ireland against the Order of the General Court in T-709/21 (action for annulment brought by WhatsApp Ireland against the EDPB's Binding Decision 1/2021, which related to WhatsApp's transparency obligations), where the General Court considered the action for annulment inadmissible.	Closed - Judgment of the European Court of Justice issued on 10 February 2026
T-682/22	Action for annulment brought by Meta Platforms Ireland against the EDPB's Binding Decision 2/2022, which related to certain processing of children's personal data by Meta Platforms Ireland Limited in the context of Instagram service.	Ongoing
T-70/23	Action for annulment brought by the Data Protection Commission against specific paragraphs of the EDPB's Binding Decision 3/2022. The case concerned the competences of the EDPB under Art. 65 GDPR.	Closed - Judgment of the General court issued on 29 January 2025 in Joined Cases T-70/23, T-84/23 and T-111/23
T-84/23	Action for annulment brought by the Data Protection Commission against specific paragraphs of the EDPB's Binding Decision 4/2022. The case concerned the competences of the EDPB under Art. 65 GDPR.	Closed - Judgment of the General court issued on 29 January 2025
T-111/23	Action for annulment brought by the Data Protection Commission against specific paragraphs of the EDPB's Binding Decision 5/2022. The case concerned the competences of the EDPB under Art. 65 GDPR.	Closed - Judgment of the General court issued on 29 January 2025
T-128/23	Action for annulment brought by Meta Platforms Ireland against the EDPB's Binding Decision 4/2022, which related to the lawfulness and transparency of the processing of personal data for behavioural advertising in the context of the Instagram service.	Ongoing

7. The EDPB also intervened in support of the EDPS in case C-413/23 P.

Case ref.	Subject matter	Status
T-129/23	Action for annulment brought by Meta Platforms Ireland against the EDPB's Binding Decision 3/2022, which related to the lawfulness and transparency of the processing of personal data for behavioural advertising in the context of the Facebook service.	Ongoing
T-153/23	Action for annulment brought by WhatsApp Ireland against the EDPB's Binding Decision 5/2022, which related to the lawfulness and fairness of the processing of personal data for service improvement in the context of the WhatsApp service.	Ongoing
T-325/23	Action for annulment brought by Meta Platforms Ireland against the EDPB's Binding Decision 1/2023, which related to the transfers of personal data outside of the EU carried out in the context of the Facebook service.	Ongoing
T-1030/23	Action for annulment brought by Tiktok Technology against the EDPB's Binding Decision 2/2023, which related to the processing of children's personal data in the context of the TikTok service, in particular with respect to certain design practices.	Ongoing
T-183/23	Action for annulment brought by a complainant against the EDPB's refusal to provide access to the file under Article 41(2) (b) of the Charter of Fundamental Rights, in relation to Binding Decision 3/2022. The EDPB's refusal was based on the lack of adverse effect of the Binding Decision on the complainant.	Closed - Judgment of the General court issued on 16 July 2025 Ruling under appeal (Case C-627/25 P)
C-627/25 P	Appeal brought by the European Commission against the ruling of the General Court in T-183/23, where the General Court considered that the right to access the file under Article 41(2)(b) of the Charter of Fundamental Rights is independent from the rights of defence and thus, it can be exercised even when the decision does not negatively affect a person.	Ongoing
T-8/24	Action for annulment brought by Meta Platforms Ireland against the EDPB's Urgent Binding Decision 1/2023, where the EDPB instructed the imposition of final measures with respect to Meta Platforms Ireland's processing of personal data for behavioural advertising under the legal bases of contract and legitimate interest.	Ongoing
T-319/24	Action for annulment and action for compensation brought by Meta Platforms Ireland against the EDPB's Opinion 8/2024, which addressed the validity of consent to process personal data for the purposes of behavioural advertising in the context of "consent or pay" models deployed by large online platforms.	Closed in 2025 - Order of the General Court issued on 29 April 2025 Order under appeal (Case C-454/25 P)
C-454/25 P	Appeal brought by Meta Platforms Ireland against the Order of the General Court in T-319/24, where the General Court considered the action for annulment inadmissible and dismissed the action for compensation for manifestly lacking any foundation in law.	Ongoing

3.3 Cooperation Under The GDPR

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

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

A case with a cross-border component is registered in a central database via the IMI. In total, 414 cross-border cases have been created in the EDPB's case register, and 1299 procedures related to the One-Stop-Shop (Art. 60 GDPR) have been triggered in 2025, out of which 572 Final Decisions.



3.4 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 2025, 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.

One Stop Shop Procedure



LSA	Lead Supervisory Authority
CSAs	Concerned Supervisory Authorities
EDPB	European Data Protection Board

STEP 1

An individual lodges a complaint or a SA opens a procedure at its own initiative or at the request of another CSA



STEP 2

LSA carries out inquiry and shares relevant information with CSAs



- LSA adopts decision on the basis of EDPB decision
- LSA sends decision to controller-processor
- The CSA with which the complaint has been lodged informs the complainant of the decision

STEP 3

LSA prepares draft decision and shares with CSAs



STEP 4

CSAs provide opinion on the draft decision; LSA takes due account of their views

LSA does not concur with objections



Case is referred to EDPB for a binding decision

Consistency Mechanism kicks in

LSA follows objections and submits revised draft decision to CSAs

CSAs have no objections

CSAs have reasoned & relevant objections

CSAs still have objections

CSAs have no further objections



- LSA adopts decision
- LSA sends decision to controller-processor
- The CSA with which the complaint has been lodged informs the complainant of the decision

Urgency Procedure (Art. 66 (1) and (2) Procedure)



DPA	Data Protection Authority
------------	---------------------------

STEP 1

A DPA can take urgent measures on its territory to protect data subjects for a maximum of 3 months.

STEP 2

2 WEEKS AS OF COMPLETENESS FILE

STEP 3



The DPA considers that final measures are necessary and requests an urgent opinion or urgent binding decision from the EDPB.

The EDPB adopts an urgent binding decision or opinion.

The EDPB is of the opinion that final measures are not necessary.

The EDPB is of the opinion that final measures are required and instructs the relevant DPA to adopt such measures.

3.5 National Cases With Exercise Of Corrective Powers

DPA's have investigative, advisory and corrective measures at their disposal to ensure entities within their countries apply data protection law correctly and consistently.

Corrective measures include the following:

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

In 2025, DPAs issued a total of 1.145.760.374 euros in fines.

DPA		Number of fines	Total Fines amount
Austria		58	€145 590
Belgium		4	€75 700
Bulgaria		81	€782 532
Croatia		13	€6 725 500
Cyprus		13	€92 500
Czech Republic		5	€141 000
Denmark		2	€13 300
Estonia		5	€3 088 100
Finland		3	€3 765 000
France		84	€486 854 500

DPA		Number of fines	Total Fines amount
Germany (all Länder grouped together)		499	€48 117 083
Greece		24	€1 582 000
Hungary		65	€255 000
Iceland		1	€33 085
Ireland		4	€530 773 000
Italy		190	€14 977 860
Latvia		5	€325 900
Liechtenstein		1	€28 846
Lithuania		5	€27 029
Luxembourg		7	€216 061
Malta		2	€22 500
Netherlands		4	€1 205 000
Norway		1	€22 000
Poland		32	€141 000
Portugal		2	€47 500
Romania		102	€437 000
Slovakia		542	€468 953
Slovenia		80	€170 020
Spain		324	€45 203 465
Sweden		3	€23 350
TOTAL			€1 145 760 374

3.6 Selection Of National Cases

The [EDPB website](#) includes a selection of DPA supervisory actions. This section of the Annual Report contains a non-exhaustive list of certain national enforcement actions in different European countries. The cases highlighted below illustrate the diverse regulatory responses to GDPR infringements, ranging from investigations and compliance orders to significant sanctions and fines.

3.6.1. Austria

- ▶ **National case and territorial scope of the GDPR**
- ▶ **Title:** Failure to comply with transparency obligations, the right of access and the right to erasure regarding the use of Microsoft 365 products in school
- ▶ **Name of controller:** Microsoft Corporation, Ministry of Education, Education Directorate, School
- ▶ **Sector:** Education
- ▶ **Legal issue:** Use of tracking cookies in Microsoft Education 365 products in the education sector (schools); distribution of roles (controllership, joint controllership); compliance with transparency obligations and the right of access and the right to erasure.
- ▶ **Timeline:** June 2024 - October 2025
- ▶ **Outcome:** Order to provide access to personal data, order to provide information under Art.13 GDPR, and order to erase cookies which are not necessary from a technical perspective.
- ▶ **Learn more:** [Read full summary](#)

3.6.2. Belgium

- ▶ **National case**
- ▶ **Title:** Reprimand for refusal to delist two URLs in Google search relating to outdated allegations
- ▶ **Name of controller:** Google LLC
- ▶ **Sector:** Digital services
- ▶ **Legal issue:** Failure to apply right to be forgotten (by not delisting links in Google Search), and lack of transparency
- ▶ **Timeline:** Decision taken on 24 April 2025
- ▶ **Outcome:** Reprimand for refusal to delist two URLs in Google search relating to outdated allegations, and for lack of transparency regarding the reasons for refusal.
- ▶ **Learn more:** [Read full summary](#)

- ▶ **National case**
- ▶ **Title:** Fine imposed on a data broker for reselling data for marketing purposes without demonstrating valid consent
- ▶ **Name of controller:** Infobel (previously “Kapitol”)
- ▶ **Sector:** Data brokers
- ▶ **Legal issue:** Unlawful reselling of personal data obtained for marketing purposes
- ▶ **Timeline:** Decision taken on 27 November 2025 (appeal pending)
- ▶ **Outcome:** 40,000 euro fine, order to erase data for which the controller does not have a valid legal basis, and order to inform recipients that the legal ground invoked is not valid.
- ▶ **Learn more:** [Read full summary](#)

3.6.3. Bulgaria

- ▶ **National case**
 - ▶ **Title:** Unlawful disclosure of personal data by the public authority Registry Agency
 - ▶ **Name of controller:** Registry Agency of Republic of Bulgaria
 - ▶ **Sector:** Public sector
 - ▶ **Legal issue:** Unlawful sharing of personal data (three names, ID number and signature) of 272 persons
 - ▶ **Timeline:** Closed: March 2025
 - ▶ **Outcome:** Fine imposed: EUR 2.556
-
- ▶ **National case**
 - ▶ **Title:** Municipality of Kyustendil Unlawfully Stored Copies of Identity Documents and Notarial Deeds
 - ▶ **Name of controller:** Municipality of Kyustendil
 - ▶ **Sector:** Public sector
 - ▶ **Legal issue:** Unlawful storage of copies of identity documents of seven natural persons who applied for access passes or car parking, resulting in their personal data were unlawfully processed.
 - ▶ **Timeline:** Closed: November 2025
 - ▶ **Outcome:** Fine imposed: EUR 2.556

3.6.4. Croatia

▶ National case

- ▶ **Title:** Mobile Banking App Processed Personal Data of Over 433,000 Users Without Legal Basis
- ▶ **Name of controller:** /
- ▶ **Sector:** Banking sector
- ▶ **Legal issue:** The bank processed the personal data of 433.922 data subjects through a software solution implemented within the mobile banking application without a legal basis under Art. 6(1), in conjunction with Art. 5(1)(a) of the GDPR. Specifically, the bank implemented a program within its mobile banking application for the Android and Huawei operating systems that scans the contents of users' mobile devices and transmits and stores, inter alia, a list of all installed applications and programs in the bank's centralised database, which constitutes a serious, excessive and unjustified interference with privacy.
- ▶ **Timeline:** December 2025
- ▶ **Outcome:** Fine imposed: EUR 1.500.000
- ▶ **Learn more:** [Read full summary](#)

▶ National case

- ▶ **Title:** Transfers of personal data to third countries without an appropriate transfer mechanism
- ▶ **Name of controller:** /
- ▶ **Sector:** Telecommunications sector
- ▶ **Legal issue:** The controller failed to conclude Standard Contractual Clauses with the processor located in the Republic of Serbia. The transfer of the data subjects' personal data to third country took place without appropriate safeguards. The processor in the Republic of Serbia was able to access the entire database with administrative privileges, which meant that it had unrestricted access rights to the personal data of 847.862 data subjects/service users of the controller. In addition, the controller failed to carry out a risk assessment for the transfer of personal data to the Republic of Serbia, which it was obliged to conduct prior to the commencement of any transfer of personal data to a third country. Such conduct is contrary to Art. 44 in conjunction with Art. 46(1) of the GDPR.
- ▶ **Timeline:** nov-25
- ▶ **Outcome:** Find imposed: EUR 4.500.000
- ▶ **Learn more:** [Read full summary](#)

3.6.5. Cyprus

▶ National case

- ▶ **Title:** Personal Data Breach Notification - Breach of Data Availability and Confidentiality
- ▶ **Name of controller:** Bank of Cyprus Public Company Limited
- ▶ **Sector:** Banking sector
- ▶ **Legal issue:** Infringement of Art. 5(1)(f), Art. 24, and Art. 32 of the GDPR
- ▶ **Timeline:** Decision taken on 5 August 2025
- ▶ **Outcome:** Administrative fine imposed: EUR 25.000

3.6.6. Czech Republic

▶ National case

- ▶ **Title:** Unlawful acces provided to client database
- ▶ **Name of controller:** /
- ▶ **Sector:** Real estate company
- ▶ **Legal issue:** Unlawful acces to a client database provided by real estate company to a third party for unsolicited marketing
- ▶ **Timeline:** June 2023 - June 2025
- ▶ **Outcome:** Fine imposed: EUR 131.000
- ▶ **Learn more:** [Read full summary](#)

3.6.7. Denmark

▶ National case

- ▶ **Title:** Investigation of DR's digital log-on procedures
- ▶ **Name of controller:** DR (Danish Broadcasting Corporation)
- ▶ **Sector:** Public institution – media enterprise
- ▶ **Legal issue:** DR's requirement that every user creates an individual account in order to stream online media content from DR, including whether DR asked for too much personal information from users
- ▶ **Timeline:** January 2025 – October 2025
- ▶ **Outcome:** The DPA did not criticise that users were asked to create a digital account with DR to be able to stream DR's online media content. The DPA did, however, reprimand DR for violating the data minimisation principle laid down in Art. 5(1)(c) GDPR, as DR required users to give their names, which were not necessary in order to create an account.
- ▶ **Learn more:** [Read full summary](#)

- ▶ **National case**
- ▶ **Title:** Violation of the storage limitation principle
- ▶ **Name of controller:** ILVA A/S
- ▶ **Sector:** Furniture company
- ▶ **Legal issue:** Violation of the storage limitation principle laid down in Art. 5 (1)(e) GDPR
- ▶ **Timeline:** 2018 - 2025
- ▶ **Outcome:** A district court had issued a fine of approx. EUR 13.300 since the court, when determining the fine, had based its decision on the net turnover of the company and not the net turnover of the corporate group which the company was a part of. The High Court submitted two preliminary questions to the Court of Justice of the European Union and on basis of the judgment of the Court of Justice the High Court decided to base its decision on the net turnover of the corporate group. Thus, the fine was increased to approx. EUR 200.700 which corresponds to the level of fine originally proposed by the DPA.
- ▶ **Learn more:** [Read full summary](#)

3.6.8. Estonia

- ▶ **National case**
- ▶ **Title:** Exposure of customer data due to inadequate security measures
- ▶ **Name of controller:** Allium UPI OÜ
- ▶ **Sector:** Wholesale of pharmaceutical and medical goods
- ▶ **Legal issue:** Infringement of Art. 5(1)(f), 24(1) and 24(2), 25(1) and 25(2), and 32(1) and 32(2) of the GDPR
- ▶ **Timeline:** February 2024 - September 2025
- ▶ **Outcome:** Fine imposed: EUR 3.000.000
- ▶ **Learn more:** [Read full summary](#)

3.6.9. Finland

- ▶ **National case**
- ▶ **Title:** Processing of personal data through tracking technologies on an online pharmacy website
- ▶ **Name of controller:** Yliopiston Apteekki
- ▶ **Sector:** Pharmacy
- ▶ **Legal issue:** Infringement of Art. 32 and 5.1.f of the GDPR (security of processing)
- ▶ **Timeline:** 2022 – May 2025
- ▶ **Outcome:** Fine imposed: EUR 1.100.000 and a reprimand issued
- ▶ **Learn more:** [Read full summary](#)

- ▶ **National case**
- ▶ **Title:** Failure in ensuring data security in the bank's authentication service
- ▶ **Name of controller:** S-Bank
- ▶ **Sector:** Banking
- ▶ **Legal issue:** Infringement of Articles 5.1.f, 25.1 and 32 of the GDPR (security of processing and data protection by design and by default)
- ▶ **Timeline:** 2022 – September 2025
- ▶ **Outcome:** Fine imposed: EUR 1.800.000 and a reprimand issued
- ▶ **Learn more:** [Read full summary](#)

3.6.10. France

- ▶ **National case**
- ▶ **Title:** Data breach
- ▶ **Name of controller:** MOBIUS SOLUTIONS LTD
- ▶ **Sector:** Software development and data analysis
- ▶ **Legal issue:** Breach to the obligation to ensure security of personal data
- ▶ **LSA:** France
- ▶ **Timeline:** November 2022 – December 2025
- ▶ **Outcome:** Administrative fine imposed: EUR 1.000.000
- ▶ **Learn more:** [Read full summary](#)

- ▶ **National case**
- ▶ **Title:** Hidden cameras
- ▶ **Name of controller:** SAMARITAINE SAS
- ▶ **Sector:** Retail
- ▶ **Legal issue:** Hidden cameras;fFailure to comply with the obligation to process data lawfully and breach of the principle of liability; failure to collect adequate, relevant and necessary data; failure to involve the Data Protection Officer in matters relating to the protection of personal data.
- ▶ **LSA:** France
- ▶ **Timeline:** August 2023 - September 2025
- ▶ **Outcome:** Administrative fine imposed: EUR 100.000
- ▶ **Learn more:** [Read full summary](#)

3.6.11. Germany (DPA Berlin)

- ▶ **National case**
- ▶ **Title:** Personalized election advertising with wrong sender
- ▶ **Name of controller:** District Association of a Party
- ▶ **Sector:** Political parties
- ▶ **Legal issue:** In order to address voters in the 2021 federal election campaign, the district association of a party received information from the registration register. The district association contacted the voters with a personalized letter. In this context, the district association misrepresented the identity of the controller under data protection law and failed to provide any data protection information. Furthermore, the district association transferred the data to a third party for mailing and printing the advertising materials without a data processing agreement.
Infringements:
 - Art. 5(1)(a) GDPR (lawfulness, fairness, transparency)
 - First sentence of Art. 6(1) (lawfulness of processing).
 - Art. 14(1), (2) and (3) GDPR (information obligations)
- ▶ **Timeline:** 2021-2025
- ▶ **Outcome:** Fine imposed: EUR 65.000

3.6.12. Germany (DPA Hamburg)

- ▶ **National case**
- ▶ **Title:** Violations concerning automated decisions in individual cases
- ▶ **Name of controller:** /
- ▶ **Sector:** Finance
- ▶ **Legal issue:** Despite good credit ratings, several customers' credit card applications were rejected through automated decision-making. These are decisions made automatically based on algorithms and without human intervention. When the affected customers subsequently requested an explanation for the rejected applications, the company failed to adequately fulfill its legally mandated information and disclosure obligations.
GDPR violations:
 - Violations of the rights of affected customers in individual cases involving automated decision-making;
 - Art. 22 GDPR
- ▶ **Timeline:** 2024-2025
- ▶ **Outcome:** Fine imposed: EUR 492.000

3.6.13. Germany (Federal DPA)

- ▶ **National case**
- ▶ **Title:** Violations in the monitoring of processors and security deficiencies in the authentication process of customers
- ▶ **Name of controller:** /
- ▶ **Sector:** Telecommunications
- ▶ **Legal issue:** The data processing carried out by partner agencies as processors for the telecommunications company has not been sufficiently monitored by the responsible provider. This made it possible for maliciously acting employees to fake contract conclusions or to make contract changes at the expense of customers.
In addition, the process of authenticating customers to the company in the combined use of the online portal and the hotline had vulnerabilities that made it possible for unauthorized third parties to access eSIM profiles.
Violations according to the GDPR:
Violations of the controller's duty of supervision over processors Art. 28(1), first sentence, GDPR, and of the requirements relating to the security of data processing Art. 32(1), GDPR.
- ▶ **Timeline:** 2019-2023, 2025
- ▶ **Outcome:** Fine imposed: EUR 15.000.000 and fine of EUR 30.000.000
- ▶ **Learn more:** [Read full summary](#)

3.6.14. Greece

- ▶ **National case**
- ▶ **Title:** Imposition of a fine on a bank for an incident of personal data breach
- ▶ **Name of controller:** National Bank of Greece S.A.
- ▶ **Sector:** Banking
- ▶ **Legal issue:** Findings of Infringement of Arts. 5.1(d), 5.1(f), 15, 25.1, 32, 33, 34 GDPR
- ▶ **Timeline:** July 2022 – January 2025
- ▶ **Outcome:** Fine imposed EUR 120.000
- ▶ **Learn more:** [Read full summary](#)

▶ **National case**

- ▶ **Title:** Imposition of fines on a telecommunications company and the data processor for personal data breach and insufficient security measures
- ▶ **Name of controller:** Vodafone S.A.
- ▶ **Sector:** Telecommunications
- ▶ **Legal issue:** Findings of Infringement of Arts. 5.1(d), 28, 29, 32 GDPR
- ▶ **Timeline:** February 2023 – June 2025
- ▶ **Outcome:** Fine imposed EUR 740.000
- ▶ **Learn more:** [Read full summary](#)

3.6.15. Hungary

▶ **National case**

- ▶ **Title:** Unlawful processing of personal data in connection with led bulb replacement program
- ▶ **Name of controller:** /
- ▶ **Sector:** Energy market
- ▶ **Legal issue:** Violations: Art. 5(1)a, c, e; 6(1); 12(1); 13(1)c,e; 13(2)a; 14(1) c,d,e; 14(2)a; 32(4); 28(3),(9) of GDPR violated through negligence.
- ▶ **Timeline:** September 2024 (but decision of the Court Spetember 2025)
- ▶ **Outcome:** Administrative Fine imposed: EUR 195.000

3.6.16. Iceland

▶ **National case**

- ▶ **Title:** Fine against the Primary Health Care of the Capital Area for the processing of personal data in the common medical records system
- ▶ **Name of controller:** /
- ▶ **Sector:** Healthcare Service Provider
- ▶ **Legal issue:** Unlawful transmission of personal data, concerning health, from medical records third parties without legal basis, through the use of shared medical record system. Violation of Arts. 5(1)(a), cf. 5(2), 6(1) and 9(1) GDPR.
- ▶ **Timeline:** Closed in February 2025
- ▶ **Outcome:** Administrative fine imposed: EUR 33.085
- ▶ **Learn more:** [Read full summary](#)

3.6.17. Ireland

▶ **National case**

- ▶ **Title:** Inquiry concerning the Department of Social Protection
- ▶ **Name of controller:** Department of Social Protection
- ▶ **Sector:** Government Department
- ▶ **Legal issue:** Processing of biometric facial templates and the use of associated facial matching technologies
- ▶ **Timeline:** July 2021 - June 2025
- ▶ **Outcome:** Formal reprimand was issued; Administrative fines imposed: EUR 550.000
An order was issued requiring the Department of Social Protection to cease processing of biometric data related to SAFE 2 registration within nine months unless a valid lawful basis can be identified.
- ▶ **Learn more:** [Read full summary](#)

▶ **Cross Border**

- ▶ **Title:** Inquiry into TikTok Technology Limited
- ▶ **Name of controller:** TikTok Technology Limited
- ▶ **Sector:** Cross-border private company
- ▶ **Legal issue:** Transfers of EEA User Data to China
- ▶ **LSA:** Ireland
- ▶ **CSA:** All SAs
- ▶ **Timeline:** Sept 2021 - April 2025
- ▶ **Outcome:** Fines imposed: EUR 530 million; An order requiring TikTok to bring its processing into compliance within six months from the period allowed for an appeal against the Decision; An order suspending TikTok's transfers within six months from the period allowed for an appeal against the Decision.
- ▶ **Learn more:** [Read full summary](#)

3.6.18. Italy

▶ **National case**

- ▶ **Title:** Activation of electricity and gas supplies based on aggressive telemarketing practices and unlawful processing of personal data
- ▶ **Name of controller:** ACEA Spa
- ▶ **Sector:** Energy market
- ▶ **Legal issue:** Unlawful use of personal data for unsolicited marketing
- ▶ **Timeline:** Closed: April 2025
- ▶ **Outcome:** Fine imposed: EUR 3.000.000
- ▶ **Learn more:** [Read full summary](#)

- ▶ **National case**
- ▶ **Title:** Failing to respond to an access request from a data subject
- ▶ **Name of controller:** Banco Bilbao Vizcaya Argentaria SA
- ▶ **Sector:** Banking
- ▶ **Legal issue:** Exercise of data subject rights
- ▶ **Timeline:** Closed: July 2025
- ▶ **Outcome:** Fine imposed: EUR 100.000
- ▶ **Learn more:** [Read full summary](#)

3.6.19. Latvia

- ▶ **National case**
- ▶ **Title:** Personal data breach affecting Latvian municipalities
- ▶ **Name of controller:** 42 Latvian municipalities
- ▶ **Sector:** Public
- ▶ **Legal issue:** Non-compliance with data controller obligations under the GDPR
- ▶ **Timeline:** 7 November 2024 – 21 November 2025
- ▶ **Outcome:** Reprimands issued and obligations imposed.
- ▶ **Learn more:** [Read full summary](#)

- ▶ **National case**
- ▶ **Title:** Failures to ensure residents' personal data security in Latvian municipalities
- ▶ **Name of controller:** PROCESSOR- LTD "ZZ DATS"
- ▶ **Sector:** Private sector – information technology (IT services)
- ▶ **Legal issue:** Non-compliance with GDPR Art. 32 (security of processing)
- ▶ **Timeline:** 7 November 2024 – 8 September 2024
- ▶ **Outcome:** Fine imposed: EUR 300.000
- ▶ **Learn more:** [Read full summary](#)

3.6.20. Liechtenstein

- ▶ **National case**
- ▶ **Title:** Teachers' access to pupils' MS Teams chats
- ▶ **Name of controller:** Department of Education
- ▶ **Sector:** Public administration/education
- ▶ **Legal issue:** Unlawful access to pupils' MS Teams chats. Parents reported that a teacher accessed their son's MS Teams chat messages on a school-provided laptop, read them, and forwarded several to her own chat. The Department of Education stated that this was not an isolated incident and relied on the performance of a public task—supervising pupils and ensuring the smooth running of classes—as the legal basis. The DPA found the access unlawful, holding that it was not necessary for those purposes, that less intrusive measures were available, and that regulations expressly permit limited private use of MS Teams chats.
- ▶ **Timeline:** 19 December 2024 - 8 July 2025
- ▶ **Outcome:** Warning and order to cease processing

3.6.21. Lithuania

- ▶ **National case**
- ▶ **Title:** Unlawful disclosure of motor vehicle roadworthiness inspection and mileage data to a third party
- ▶ **Name of controller:** Lithuanian Association of Technical Inspection Enterprises "TRANSEKSTA"
- ▶ **Sector:** Transport
- ▶ **Legal issue:** A complaint concerning the unlawful disclosure of the complainant's personal data (motor vehicle roadworthiness inspection and mileage data) to a third party, in breach of Art. 5(1)(a) (the principle of lawfulness) and the requirements of Art. 6(1) of the GDPR.
- ▶ **Timeline:** 18 November 2025
- ▶ **Outcome:** The complaint was upheld, and the data controller was ordered immediately to cease the disclosure of personal data relating to the complainant to the company until the relevant processing operations are brought into compliance with the requirements of Art. 6(1) of the GDPR.
- ▶ **Learn more:** [Read full summary](#)

▶ National case

- ▶ **Title:** Repeated retrieval of personal data from the Real Property Register by a municipal administration without a valid legal basis
- ▶ **Name of controller:** A municipal administration (local self-government authority), acting as a recipient of data from the Real Property Register
- ▶ **Sector:** Public administration
- ▶ **Legal issue:** Unlawful processing of personal data through repeated retrieval of Real Property Register extracts containing personal data, in breach of Art. 5(1)(a) and Art. 6(1) GDPR; failure to ensure data protection by design under Art. 25 GDPR.
- ▶ **Timeline:** 12 September 2025
- ▶ **Outcome:** The controller was ordered to ensure that, when performing functions for which it is necessary to obtain data from the Real Property Register but not necessary to process personal data, personal data are not processed, including their retrieval. The DPA also initiated GDPR monitoring actions against the Centre of Registers in order to ensure compliance with Art. 25 GDPR.
- ▶ **Learn more:** [Read full summary](#)

3.6.22. Luxembourg

- ▶ **Cross-border case**
- ▶ **Name of controller:** N/A
- ▶ **Sector:** Financial institution
- ▶ **Legal issue:** Respect of the response deadlines according to Arts. 12 (3) and (4) GDPR concerning the requests of data subjects
- ▶ **Outcome:** 1. Reprimand according to Art. 58 (2) (b) GDPR because of a violation of Arts. 12 (3) and (4) GDPR;
2. An administrative fine according to Art.58 (2) (i) of EUR 175.000 for the violation of Arts. 12 (3) and (4) GDPR.

▶ National case

- ▶ **Title:** N/A
- ▶ **Name of controller:** N/A
- ▶ **Sector:** Public body (School)
- ▶ **Legal issue:** Video-surveillance on school premises. 1. Violation of the Arts. 5 (2), 5 (1) (a) linked to Art. 13 (1) and 13 (2), 5 (1) (c), 5(1) (e) and 32 (1) GDPR.
- ▶ **Timeline:** /
- ▶ **Outcome:** 1. Reprimand according to Art. 58 (2) (b) of the GDPR;
3. An order to bring processing operations into compliance (Art. 58 (2) (d) of the GDPR) with Arts. 13 (1) and (2) of the GDPR;
4. An order to bring processing operations into compliance (Art. 58 (2) (d) of the GDPR) with Art. 5 (1) (c) of the GDPR;
5. An order to bring processing operations into compliance (Art. 58 (2) (d) of the GDPR) with Art. 5 (1) (e) of the GDPR; and
6. An order to bring processing operations into compliance (Art.58 (2) (d) of the GDPR) with Art.32 (1) of the GDPR.

3.6.23. Malta

- ▶ **National case**
- ▶ **Title:** Unlawful compulsory collection of mobile numbers for online payments
- ▶ **Name of controller:** /
- ▶ **Sector:** Government appointed body, service provider
- ▶ **Legal issue:** Failure to comply with the data minimisation principle
- ▶ **Timeline:** 14 May 2025 – 4 December 2025
- ▶ **Outcome:** Reprimand and order to take action to comply with the data minimisation principle
- ▶ **Learn more:** [Read full summary](#)

▶ **National case**

- ▶ **Title:** Infringements of GDPR Principles, Data Subject Rights and DPO Obligations
- ▶ **Name of controller:** /
- ▶ **Sector:** Healthcare service provider
- ▶ **Legal issue:** Infringement of Arts.5(1)(a), 5(1)(d), 6(1), 14, 16(1) and 37(1)(c) GDPR
- ▶ **Timeline:** 5 July 2024 – 4 February 2025
- ▶ **Outcome:** The Commissioner issued a reprimand, ordered the controller to rectify inaccurate data, erase unlawfully obtained data and designate a Data Protection Officer (DPO) within 20 days, and imposed administrative fines totalling EUR 20.000 for multiple GDPR infringements relating to lawfulness, fairness and transparency, rectification and failure to designate a DPO.
- ▶ **Learn more:** [Read full summary](#)

3.6.24. Netherlands

- ▶ **National case**
- ▶ **Title:** Unlawful processing by a municipality
- ▶ **Name of controller:** /
- ▶ **Sector:** Government
- ▶ **Legal issue:** Further processing of personal data without a legal basis
- ▶ **Timeline:** October 2021 – February 2025
- ▶ **Outcome:** Fine imposed: EUR 300.000

3.6.25. Norway

- ▶ **National case**
- ▶ **Title:** Unlawful sharing of personal information through tracking pixels
- ▶ **Name of controller:** 116111.no (Municipality of Kristiansand), apotekfordeg.no (Apotekfordeg AS), bibel.no (Det norske bibelselskap), drdropin.no (Dr. Dropin AS), ifengsel.no (Kirkens Bymisjon), nhi.no (Norsk Helseinformatikk AS).
- ▶ **Sector:** Public, private and non-profit
- ▶ **Legal issue:** Unlawful sharing of personal data about website visitors to third parties without legal basis
- ▶ **Timeline:** Closed: June 2025
- ▶ **Outcome:** One fine of EUR 22 000 and five reprimands.
- ▶ **Learn more:** [Read full summary](#)

3.6.26. Portugal

- ▶ **National case**
- ▶ **Title:** Russiagate – Lisbon City Council fine for GDPR violations (Portuguese DPA Decision 1569/2021)
- ▶ **Name of controller:** Lisbon City Council
- ▶ **Sector:** Public Administration / Local Government
- ▶ **Legal issue:** The CNPD initiated an investigation following a complaint from two citizens regarding the transmission of their personal data to the Russian Embassy.
Violation of several GDPR principles and obligations, namely: • Principle of lawfulness, fairness and transparency (Art. 5(1)(a) GDPR); • Principle of data minimisation, in its need-to-know dimension (Art. 5(1)(c) GDPR); • Failure to provide information to data subjects (Art. 13 GDPR); • Violation of the principle of storage limitation; • Failure to carry out a Data Protection Impact Assessment (DPIA); • Processing of personal data without an appropriate legal basis (Arts. 6 and 9 GDPR).
These infringements consisted of 130 administrative offences, committed intentionally, in material authorship and in a completed form.
- ▶ **Timeline:**
 - 21 December 2021 – CNPD's Decision 1569/2021 imposing the fine in the amount of €1,250,000.
 - Later date - Judicial appeal lodged by the Lisbon City Council
- ▶ **Outcome:**
 - The Lisbon City Council was found liable for 130 infringements of the GDPR;
 - A single administrative fine of €738,000.00 was confirmed by the Superior Court (following a reassessment from the initial fine of €1.250.000);
 - Multiple core GDPR principles were found to have been breached, including lawfulness, data minimisation, transparency, storage limitation and the obligation to carry out a DPIA.
- ▶ **Learn more:** [Read full summary](#)

3.6.27. Romania

▶ Cross-border case

- ▶ **Title:** Notification of Personal Data Breach Art. 33, Art. 34
- ▶ **Name of controller:** Klass Wagen S.R.L.
- ▶ **Sector:** Cars rent
- ▶ **Legal issue:** Personal data breach (Articles 33 and 34)
- ▶ **LSA:** Romania
- ▶ **CSA:** Germany (Baden-Württemberg), Italy, Slovakia; Germany (Hessen), Netherlands, Ireland, Hungary, Germany (Rhineland-Palatinate), Spain, Austria, Bulgaria, France, Denmark; Germany (Bavaria – Private Sector)
- ▶ **Timeline:** January 2025 - October 2025
- ▶ **Outcome:** One administrative fine and one corrective measure
- ▶ **Learn more:** [Read full summary](#)

▶ Cross-border case

- ▶ **Title:** Participating in opinion polls in exchange for rewards
- ▶ **Name of controller:** Data Diggers Market Research SRL
- ▶ **Sector:** Electronic communications
- ▶ **Legal issue:** Information, right of access, lawfulness of the processing
- ▶ **LSA:** Romania
- ▶ **CSA:** France, Italy, Netherlands, Sweden, Germany (Bavaria) and Poland
- ▶ **Timeline:** February 2023 - April 2025
- ▶ **Outcome:** Three administrative fines and one corrective measure
- ▶ **Learn more:** [Read full summary](#)

3.6.28. Slovakia

▶ National case

- ▶ **Title:** Submission by an advocate representing data subjects in a criminal case
- ▶ **Name of controller:** Regional Office of the Prosecutor in Nitra
- ▶ **Sector:** Law enforcement authorities
- ▶ **Legal issue:** Transfer of personal data relating to six data subjects—other than the advocate, who had represented some of them in criminal proceedings—originally processed in the context of a procedural act under the Law Enforcement Directive (LED) regime, to an independent professional self-governing body (the Slovak Bar Association) in the form of a complaint concerning the advocate’s unethical statements, without anonymising the personal data of those data subjects who had no connection to the alleged misconduct.
- ▶ **Timeline:** 27 April 2025 - 8 October 2025
- ▶ **Outcome:** Measure imposed to adopt internal organisational measures and procedures to prevent the processing of personal data of data subjects originally processed for the performance of tasks for the purposes of criminal proceedings pursuant to Section 3(3) of Act No. 18/2018 Coll. for other purposes falling under any of the conditions set out in Art.6(1) GDPR, without a prior purpose compatibility assessment pursuant to Art. 6(4) GDPR.

▶ National case

- ▶ **Title:** Inadequate handling of a right of access request sent to a mobile network operator simultaneously via the communication channel designated for complaints and the communication channel designated for the exercise of rights under the GDPR
- ▶ **Name of controller:** Orange Slovensko, a.s.
- ▶ **Sector:** Mobile network operator services
- ▶ **Legal issue:** Assessing the scope of the controller’s response in which it simultaneously addressed a complaint using an analysis of the applicant’s received calls and, at the same time, informed the applicant that it does not process his telephone number. By responding in this manner, the controller acted in breach of the GDPR, as it falsely claimed not to have identified calls from the applicant, even though its analysis of those calls was set out in the same written document.
- ▶ **Timeline:** 27 December 2024 - 06 May 2025
- ▶ **Outcome:** Fine imposed: EUR 3,000

3.6.29. Slovenia

▶ National case

- ▶ **Title:** Employee surveillance through monitoring software
- ▶ **Name of controller:** RIEDL PRECISION d.o.o.
- ▶ **Sector:** Manufacturing
- ▶ **Legal issue:** Processing of personal data (monitoring software) in the employment context
- ▶ **Timeline:** Closed: December 2025
- ▶ **Outcome:** Fine imposed: EUR 71.474

▶ National case

- ▶ **Title:** Video surveillance in a rental apartment
- ▶ **Name of controller:** Oddaja sob (sole entrepreneur)
- ▶ **Sector:** Accommodation brokerage
- ▶ **Legal issue:** Processing of personal data through the unlawful installation of a surveillance camera in an apartment
- ▶ **Timeline:** Closed: May 2025
- ▶ **Outcome:** Fine imposed: EUR 16.000

3.6.30. Spain

▶ National case

- ▶ **Title:** Use of biometric data for airport access
- ▶ **Name of controller:** AENA, S.M.E., S.A.
- ▶ **Sector:** Airport and air traffic sector
- ▶ **Legal issue:** Facial recognition identification system for controlling passenger access to certain areas of airports without justifying its necessity and proportionality
- ▶ **Timeline:** April 2023 – November 2025
- ▶ **Outcome:** Fine imposed: EUR 10.043.002, and temporary suspension of all biometric data processing until AENA carries out a Data Protection Impact Assessment (DPIA) in accordance with Art. 35 GDPR.
- ▶ **Learn more:** [Read full summary](#)

▶ National case

- ▶ **Title:** Repeated data breaches and GDPR security failures
- ▶ **Name of controller:** CENTROS COMERCIALES CARREFOUR, S.A.
- ▶ **Sector:** Retail and E-commerce
- ▶ **Legal issue:** Infringement of the principle of integrity and confidentiality, failure to implement appropriate technical and organizational security measures and inadequate communication of data breaches to the affected data subjects.
- ▶ **Timeline:** May 2023 – March 2025
- ▶ **Outcome:** Fine imposed: EUR 3.200.000, and the communication of personal data breaches to the affected parties whose data has been affected in the terms and conditions provided for by Art. 34 GDPR.
- ▶ **Learn more:** [Read full summary](#)

3.6.31. Sweden

▶ National case

- ▶ **Title:** Lack of security in web form for reporting discrimination
- ▶ **Name of controller:** The Equality Ombudsman
- ▶ **Sector:** Government agency
- ▶ **Legal issue:** Insufficient security measures in web form used for tips and complaints regarding discrimination
- ▶ **Timeline:** October 2021 – April 2025
- ▶ **Outcome:** Fine imposed: EUR 9.000
- ▶ **Learn more:** [Read full summary](#)

▶ National case

- ▶ **Title:** Wrongdoing by political parties to send political information without consent
- ▶ **Name of controller:** The Moderate Party and the Sweden Democrats
- ▶ **Sector:** Political parties
- ▶ **Legal issue:** Sending political information via SMS or email to private citizens without their consent
- ▶ **Timeline:** Moderate Party: March 2023– October 2025; Sweden Democrats: July 2024 – October 2025
- ▶ **Outcome:** Reprimands to both parties
- ▶ **Learn more:** [Read full summary](#)

4. Annexes



4.1 General guidance and recommendations


- ▶ Guidelines 1/2025 on pseudonymisation - Adopted on 16 January 2025
- ▶ Guidelines 02/2025 on processing of personal data through blockchain technologies - Adopted on 08 April 2025
- ▶ Guidelines 3/2025 on the interplay between the DSA and the GDPR - Adopted on 11 September 2025
- ▶ Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation - Endorsed on 9 October 2025
- ▶ Guidelines 02/2024 on Article 48 GDPR - Adopted on 4 June 2025 (Final version adopted after public consultation)
- ▶ Recommendations 1/2025 on the 2027 WADA World Anti-Doping Code - Adopted on 11 February 2025
- ▶ Recommendations 2/2025 on the legal basis for requiring user account creation on e-commerce websites - Adopted on 03 December 2025

4.2 Consistency opinions

- ▶ Opinion 01/2025 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Coface Group - Adopted on 16 January 2025
- ▶ Opinion 2/2025 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of the Alfa

Laval Group - Adopted on 13 March 2025

- ▶ Opinion 3/2025 on the draft decision of the French Supervisory Authority (FR SA) regarding the “Lexing GDPR certification criteria” - Adopted on 8 April 2025
- ▶ Opinion 4/2025 on the draft decision of the Finnish Supervisory Authority regarding the Controller Binding Corporate Rules of the Nokia Group - Adopted on 8 April 2025
- ▶ Opinion 5/2025 on the draft decision of the Finnish Supervisory Authority regarding the Processor Binding Corporate Rules of the Nokia Group - Adopted on 8 April 2025
- ▶ Opinion 8/2025 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of the Statkraft Group - Adopted on 5 May 2025
- ▶ Opinion 9/2025 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the Worldline Group - Adopted on 5 May 2025
- ▶ Opinion 10/2025 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Worldline Group - Adopted on 5 May 2025
- ▶ Opinion 11/2025 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the Signify Group - Adopted on 4 June 2025
- ▶ Opinion 12/2025 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the ASML Group - Adopted on 4 June 2025
- ▶ Opinion 13/2025 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the Aramex Group - Adopted on 8 July 2025

- 
- ▶ Opinion 14/2025 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of the Wilh. Wilhelmsen Group - Adopted on 8 July 2025
 - ▶ Opinion 15/2025 on the draft decision of the Austrian Supervisory Authority (AT SA) regarding the certification criteria of BDO Consulting GmbH - Adopted on 8 July 2025
 - ▶ Opinion 16/2025 regarding the draft decision of the German North Rhine Westphalia Supervisory Authority regarding Trusted Site Data Privacy (TÜV IT) certification criteria - Adopted on 8 July 2025
 - ▶ Opinion 28/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by Brazil - Adopted on 4 November 2025
 - ▶ EDPB-EDPS Joint Opinion 01/2025 on the Proposal for a Regulation on simplification measures for SMEs and SMCs, in particular the record-keeping obligation under Art. 30(5) GDPR - Adopted on 8 July 2025
 - ▶ Statement 1/2025 on Age Assurance - Adopted on 11 February 2025
 - ▶ Statement 2/2025 on the implementation of the PNR Directive in light of CJEU Judgment C-817/19 - Adopted on 13 March 2025
 - ▶ Statement 4/2025 on the European Commission's Recommendation on draft non-binding model contractual terms on data sharing under the Data Act - Adopted on 8 July 2025

4.3 Legislative consultation

- ▶ Opinion 06/2025 regarding the extension of the European Commission Implementing Decisions under the GDPR and the LED on the adequate protection of personal data in the United Kingdom (Art.70) - Adopted on 5 May 2025
- ▶ Opinion 07/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the European Patent Organisation (Art.70) - Adopted on 5 May 2025
- ▶ Opinion 26/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom - Adopted on 16 October 2025
- ▶ Opinion 27/2025 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data by the United Kingdom - Adopted on 16 October 2025

4.4 Other documents

- ▶ Position paper on Interplay between data protection and competition law - Adopted on 16 January 2025
- ▶ Report on the use of SPE external experts in 2024 - Adopted on 13 March 2025

Postal address

Rue Wiertz 60, B-1047 Brussels

Office address

Rue Montoyer 30, B-1000 Brussels



European
Data Protection
Board



edpb.europa.eu