EDPS

EUROPEAN
DATA PROTECTION
SUPERVISOR

ANNUAL REPORT
2025

An executive summary of the Annual Report 2025, which gives an overview of the key developments of EDPS activities in 2025, is also available.

Further details about the EDPS can be found on our website edps.europa.eu

The website also details a subscription feature to our newsletter.

Manuscript completed in February 2026

Luxembourg: Publications Office of the European Union, 2026

PRINT ISBN 978-92-9242-956-0 ISSN 1830-5474 doi:10.2804/8714957 QT-01-25-005-EN-C

PDF ISBN 978-92-9242-955-3 ISSN 1830-9585 doi:10.2804/8968388 QT-01-25-005-EN-N

Table of Contents

FOREWORD

It is my privilege to present the EDPS Annual Report 2025 – a year defined by the transition from strategic preparation to robust operationalisation across our expanding mandate.

If 2024 was a year of taking stock and celebrating our history, 2025 has been about delivering concrete results in an increasingly complex digital landscape. Our work this year has been driven by a commitment to ensuring that the fundamental rights of individuals continue to be protected within the ambitious and evolving Digital Rulebook.

A defining feature of 2025 has been the rapid evolution of our role in Artificial Intelligence. Our newly established AI Unit has moved from foundational planning to active mapping and governance. We have mapped the AI ecosystem across EU institutions, bodies, offices and agencies (EUIs), identifying growing use of generative AI and increasing reliance on off-the-shelf tools, underscoring the vital need for institutional accountability in this area. To support innovation within safe boundaries, we launched an AI regulatory sandbox pilot project, providing a collaborative space for EUIs to test AI systems under the guidance of the regulator before they are deployed.

Our commitment to technological foresight remains a cornerstone of our mission. Through the Technology and Privacy Unit, we have analysed the risks and opportunities of emerging trends such as Agentic AI, AI companions and federated learning. Furthermore, 2025 marked a significant expansion of our responsibilities in the field of cybersecurity. As a permanent member of the Inter-Institutional Cybersecurity Board, the EDPS is now playing a central role in strengthening the digital defences of the EU administration.

In the realm of Policy and Legislative Consultation, we reached a record level of activity, responding to 145 legislative consultations. Our advice has spanned critical topics from digital identity to targeted modifications to the GDPR, always aiming to ensure that new laws are legally sound and aligned with EU values. We also fostered a high-level debate on competition and innovation to ensure that the Digital Rulebook is implemented coherently across different regulatory sectors.

Our Supervision and Enforcement Unit has doubled down on ensuring accountability, notably through our landmark investigation into the European Commission's use of Microsoft 365 and our scrutiny of international data transfers. Whether defending our decisions before the Court of Justice of the European Union or auditing large-scale IT systems like the Visa Information System and Eurodac, our focus remains on the practical application of data protection standards.

2025 was a foundational year for our upcoming role as a market surveillance authority (MSA) and notified body for EUIs under the AI Act. In anticipation of the August 2026 deadline for high-risk AI provisions, we prioritised a strict 'functional separation' between these new responsibilities and our core data protection mandate. By investing in specialised expertise and closely following the development of harmonised standards, we continued building operational readiness to supervise AI in sensitive sectors such as law enforcement and migration. Our objective is to replace regulatory uncertainty with a coherent framework that provides legal certainty for the EU administration while robustly safeguarding fundamental rights.

Finally, our achievements this year demonstrate the power of collaboration. Through the European Data Protection Board and international networks like the Global Privacy Assembly, the G7 DPAs roundtable, and the International Organisations Workshop on Data Protection, we continue to advocate for high privacy standards that transcend borders.

The digital future is here, and while we cannot eliminate every risk, the EDPS is fully equipped to guide the EU administration through this transformation with expertise, independence and unwavering focus on the rights of the citizen.

Wojciech Wiewiórowski
European Data Protection Supervisor

CHAPTER ONE

ABOUT US

1.1. The EDPS

1.1.1. Who we are

The European Data Protection Supervisor (EDPS) is the European Union's independent data protection authority responsible for supervising the processing of personal data by the European institutions, bodies, offices and agencies (EUIs).

We advise EUIs on new legislative proposals and initiatives related to the protection of personal data.

We monitor the impact of new technologies on data protection and cooperate with supervisory authorities to ensure the consistent enforcement of EU data protection rules.

Additionally, since the entry into force of the AI Act, we ensure that the EU institutions use, develop, and deploy AI in line with its rules.

1.1.2. Our mission

Data protection is a fundamental right, protected by EU law. We promote a strong data protection culture within EUIs.

We carry out our work according to the following four values and principles.

- **Impartiality:** Working within the legislative and policy framework given to us, being independent and objective, finding the right balance between the interests at stake.
- **Integrity:** Upholding the highest standards of behaviour and to always do what is right.
- **Transparency:** Explaining what we are doing and why, in clear language that is accessible to all.
- **Pragmatism:** Understanding our stakeholders' needs and seeking solutions that work in a practical way.

1.1.3. What we do

We have five main fields of work.

- **Supervision and Enforcement:** Monitoring the processing of personal data by EUIs to ensure that they comply with data protection rules.
- **Policy and Legislative Consultation:** Advising the European Commission, the European Parliament and the Council of the European Union on legislative proposals and initiatives related to data protection.
- **Technology and Privacy:** Monitoring and assessing technological developments impacting the protection of personal data. We oversee that the systems supporting the processing of personal data by EUIs implement adequate safeguards to ensure compliance with data protection rules. We implement the digital transformation of the EDPS.
- **AI Preparedness:** Under the AI Act we act as notified body and market surveillance authority to assess the conformity of high-risk AI systems that are developed, deployed and used by EUIs. We ensure that the use, development and deployment of AI by EUIs is coherent and consistent with the AI Act. Our responsibilities embody the principles of good governance, risk management and supervision.
- **Cooperation:** Working with data protection authorities to promote consistent data protection across the EU and European Economic Area. Our main platform for cooperation with data protection authorities is the European Data Protection Board, to whom we provide a secretariat and have a Memorandum of Understanding defining how we work together.

Each area of expertise, enumerated above, is embodied by Units and Sectors that bring together a diverse group of legal and technical experts, as well as other specialists in their field from all across the European Union.

1.1.4. Our powers

The powers we have as the data protection authority of EUIs are laid out in Regulation (EU) 2018/1725.

Under this regulation, we can, for example, warn or reprimand an EUI that is unlawfully or unfairly processing personal data, order EUIs to comply with requests to exercise individuals' rights, impose a temporary or definitive ban on a particular data processing operation, impose administrative fines to EUIs, or refer a case to the Court of Justice of the European Union.

We also have specific powers to supervise the way the following EUIs process personal data:

- Europol (the EU Agency for Law Enforcement Cooperation), under Regulation 2016/794;

- Eurojust (the EU Agency for Criminal Justice Cooperation), under Regulation 2018/1727;

- EPPO (the European Public Prosecutor's Office), under Regulation 2017/1939;

- Frontex (the European Border and Coast Guard), under Regulation 2019/1896.

Since 2024, the EDPS has acquired new powers and roles under the AI Act: notified body and market surveillance authority to assess the conformity of high-risk AI systems that are developed, deployed and used by EUIs.

1.2. EDPS Strategy 2020-2024

In a connected world, where data flows across borders, solidarity within Europe and internationally will help to strengthen the right to data protection and make data work for people across the EU and beyond.

Wojciech Wiewiórowski was appointed as Supervisor by a joint decision of the European Parliament and the Council to serve a five-year term, beginning on 6 December 2019. In 2025, the selection procedure for a new EDPS mandate for the next term of five years was still ongoing. Pending a renewed mandate the **EDPS Strategy for 2020-2024** continued to guide our work.

The strategy focuses on three pillars: Foresight, Action and Solidarity, to shape a safer, fairer and more sustainable digital future.

- **Foresight:** Our commitment to being a smart institution that takes the long-term view of trends in data protection and the legal, societal and technological context.

- **Action:** Proactively develop tools for EUIs to be world leaders in data protection. To promote coherence in the activities of enforcement bodies in the EU with a stronger expression of genuine European solidarity, burden sharing and common approach.

- **Solidarity:** Our belief is that justice requires privacy to be safeguarded for everyone, in all EU policies, whilst sustainability should be the driver for data processing in the public interest.

For more information about the EDPS, please consult our Frequently Asked Questions page on the EDPS website.

For more information about data protection in general, consult our Glossary page on the EDPS website.

CHAPTER TWO

HIGHLIGHTS OF 2025

During 2025, we continued to deliver on our actions to shape a safer digital future, operating in our core areas of expertise: Supervision and Enforcement, Policy and Legislative Consultation, Technology and Privacy, and Artificial Intelligence.

In the area of Supervision and Enforcement, we:

- advised European institutions, bodies, offices and agencies (EUIs) on planned or existing processing operations in the form of supervisory opinions on joint controllership in banking supervision, transparency in internal investigations and the implementation of the European Travel Information and Authorisation System (ETIAS) watchlist;
- investigated alleged breaches of data protection laws by EUIs, such as the European Commission's use of Microsoft 365, international transfers under cloud service contracts, and the independence and dismissal of Data Protection Officers;
- audited EUIs to identify strengths and weaknesses in their data protection practices, for example in the processing of health data, epidemic intelligence and the use of mobile applications;
- addressed complaints from individuals who believe that an EUI has infringed their data protection rights, including in the context of staff data transmissions to Permanent Representations and access to selection board records;

- defended privacy and the EDPS' institutional role and decisions before the Court of Justice of the European Union, notably regarding the definition of personal data and the EDPS' legal standing;
- collaborated with Data Protection Officers of EUIs to uphold consistent and coherent data protection standards across EU public administration with the organisation of bi-annual meetings and focused roundtables;
- completed supervisory work in three key areas: the EU interoperability framework, safeguards for international data transfers and the application of Data Protection Impact Assessments.

In the area of Policy and Legislative Consultation, we:

- issued 145 responses to legislative consultation requests from the European Commission in the form of opinions, formal and informal comments, providing advice on the data protection implications of draft EU laws and international agreements on a range of topics, including Justice and Home Affairs, digital ID and credentials, targeted modifications of the General Data Protection Regulation (GDPR), and international agreements on tax compliance;
- actively contributed to promoting and further developing consistent and coherent data protection rules and practices across the EU, in particular through our membership in the European Data Protection Board (EDPB) and by fostering cooperation between competent digital regulators to ensure the effective implementation of the EU's Digital Rulebook;
- fostered international and institutional cooperation to promote high data protection standards, for instance by organising a high-level debate on competition, innovation and data protection to reflect on the impact of the EU's Digital Rulebook on the rights of citizens.

In the area of Technology and Privacy, we:

- forecasted and analysed digital and technological developments, highlighting their opportunities and risks in our publications and podcasts of TechSonar and TechDispatch, with a focus on AI-related technologies, federated learning and digital identity wallets;
- organised our Internet Privacy Engineering Network (IPEN) on secure multi-party computation;
- helped EUIs address, overcome and prevent data breaches through awareness campaigns and the PATRICIA II tabletop exercise, receiving international recognition for these initiatives at the Global Privacy Assembly Awards in the Accountability category;
- audited IT systems of EUIs, from websites through our awareness campaign pilot, to Large Scale IT Systems, such as the Visa Information System, Eurodac and the Customs Information System;
- pursued our actions for digital transformation, such as launching the Website Evidence Collector as an online service (WEC Online) and streamlining the institution's IT infrastructure and support;
- prepared for the EDPS's evolving role in cybersecurity as a permanent member of the Inter-Institutional Cybersecurity Board and by improving the institution's preparedness with new maturity and risk assessments;
- issued new AI risk management guidance to assist EUIs in identifying and mitigating technical risks associated with the development and deployment of AI systems.

Supporting internal governance mechanisms and compliance involved:

- adopting a decision on transparency measures at the EDPS, and having it referenced in the website of the interinstitutional Transparency Register;
- adopting a decision on records and archives management at EDPS;
- handling 72 requests for access to documents, the highest number so far, and a sign of the growing interest in the EDPS's activities;
- the DPO providing independent advice to internal services, as delegated controllers, with a view to ensure the EDPS's accountability;
- the AI Correspondent facilitating the EDPS's compliance with the AI Act.

In the area of Artificial Intelligence, we:

- reinforced the newly established AI Unit to prepare for the EDPS's tasks as market surveillance authority and notified body of EUIs' AI systems under the AI Act;
- mapped the current AI ecosystem in relation to prohibited practices and high-risk systems within EUIs, publishing a report that highlights the dominant areas of AI use and potential enforcement priorities for the EDPS;
- launched an AI regulatory sandbox pilot project to offer safe and collaborative environment for EUIs to develop and test innovative AI systems under regulatory oversight;
- strengthened the AI Act Correspondents Network (AIACN) via meetings and workshops to enable capacity-building and knowledge exchange between EUIs as they prepare to comply with the AI Act;
- enhanced cooperation with EU (national) market surveillance authorities and international organisations in the area of AI governance and supervision;
- actively contributed to the implementation and consistent and effective application of the AI Act by participating in interinstitutional fora and working groups, and submitting to public consultations.

In communicating data protection, we:

- expanded and diversified our online presence by using a broader range of tools, formats and targeted campaigns to reach key audiences more effectively;
- reinforced our social media mix by reactivating our presence on Mastodon, a decentralised and privacy-oriented platform aligned with our values;
- organised and contributed to events to increase the visibility of our work and promote high data protection standards at global level;
- maintained and further developed relationships with journalists, stakeholders and the public;
- strengthened the EDPS's visibility as an employer, enhancing its attractiveness through targeted employer branding initiatives.

As a working organisation, we:

- managed human and financial resources in a sustainable way to deliver our mandate and tasks;
- invested in employees, Units and Sectors by offering trainings and development opportunities.

2.1. Key performance indicators 2025

We use a number of key performance indicators (KPIs) to help us monitor our performance in light of the main objectives set out in the EDPS Strategy. This ensures that we are able to adjust our activities, if required, to increase the impact of our work and the effective use of resources.

The KPI scoreboard contains a brief description of each KPI and the results on 31 December 2025. These results are measured against initial targets, or against the results of the previous year, used as an indicator.

In 2025, we met or surpassed the targets set in all KPIs, except one, confirming the positive trend in implementing our strategic objectives throughout the year. KPI 7, on followers on EDPS social media, did not fully meet the set target, as our social media platforms have reached a stage of maturity and audience saturation, where growth has naturally stabilised and is no longer as dynamic as in previous years. On the other hand, in 2025, we reactivated the EDPS Mastodon account, previously operating as EU Voice, which had been closed in May 2024 following the conclusion of its pilot phase. This initiative aimed to reintroduce an alternative communications tool in support of a more democratic, decentralised and privacy-friendly model of social media and allowed us to reconnect with the 6,200 followers already gathered under the former EU Voice account.

Table 1
Key performance indicators 2025

	KEY PERFORMANCE INDICATORS	RESULTS 31.12	TARGET 2025
	**KPI 1** **Internal Indicator** Number of cases, incl. publications, on technology monitoring and on promoting technologies to enhance privacy and data protection organised or co-organised by the EDPS.	7 cases	5 cases
	**KPI 2** **Internal & External Indicator** Number of activities focused on cross-disciplinary policy solutions (internal & external).	8 activities	8 activities
	**KPI 3** **Internal Indicator** Number of cases dealt with in the context of international cooperation (GPA, CoE, OECD, GPEN, IWGDPT, Spring Conference, international organisations) for which the EDPS has provided a substantial written contribution.	34 cases	10 cases
	**KPI 4** **External Indicator** Number of files for which the EDPS acted as a lead rapporteur, rapporteur, or a member of the drafting team in the context of the EDPB.	22 files	10 files
	**KPI 5** **External Indicator** Number of Article 42 Opinions and Joint EDPS-EDPB Opinions issued in response to the European Commission's legislative consultation requests.	31 opinions	25 opinions
	**KPI 6** **External Indicator** Number of audits/visits carried out physically or remotely.	6 audits	5 audits
	**KPI 7** **External Indicator** Number of followers on the EDPS social media accounts.	LinkedIn: 90,838 X: 28,102 Youtube: 3,681 Instagram: 731 Total: 123,352 *Mastodon*: 6,211	2024 figures (+10%) LinkedIn: 82,881 (91,169) X: 28,860 (31,746) YouTube: 3,409 (3,750) Instagram: 314 (345) Total: 115,464 (127,010)
	**KPI 8** **Internal Indicator** Occupancy rate of establishment plan.	92.50%	90%
	**KPI 9** **Internal Indicator** Budget implementation.	92.50%	90%

CHAPTER THREE

SUPERVISION AND ENFORCEMENT

One of our core tasks is to supervise the way EU institutions, bodies and agencies (EUIs) process individuals' personal data, to ensure their compliance with the applicable data protection law. This task is carried out by the EDPS's Supervision and Enforcement Unit (S&E Unit).

To ensure EUIs' compliance with the applicable data protection law, we use the various tools and powers at our disposal, mainly under Regulation (EU) 2018/1725 (the Data Protection Regulation for EUIs). This includes:

- issuing supervisory opinions, in which we provide advice to EUIs on their planned or existing data processing operations;
- issuing decisions to authorise transfers of personal data from EUIs to third countries and international organisations;
- carrying out data protection audits to verify their compliance;
- conducting investigations following a complaint or on our own initiative, when their are indications that EUIs infringed data protection law;
- using the EDPS's corrective powers, including administrative fines and litigation in the EU courts;
- cooperating with the data protection officers (DPOs) of the EUIs to promote a strong data protection culture and support their independence.

Part of the S&E Unit's work is therefore dedicated to monitoring and supervising the EUIs operating in the Area of Freedom, Security and Justice (ASFJ):

- the European Union Agency for Law Enforcement Cooperation (Europol);
- the European Union Agency for Criminal Justice Cooperation (Eurojust);

- the European Public Prosecutor's Office (EPPO);
- the European Union Agency for Asylum (EUAA);
- the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA).

This role extends across a broad range of policy areas, including border management, asylum and immigration, police cooperation, the fight against serious crime, and judicial cooperation in civil and criminal matters.

This section presents the key supervisory and enforcement activities carried out in 2025. Throughout the year, we continued to support EUIs in applying EU data protection rules consistently and effectively, while addressing emerging risks linked to technological developments and complex processing operations.

3.1. Supervisory opinions

Supervisory opinions are a core instrument through which we support EUIs in ensuring that planned or existing processing operations comply with EU data protection rules. By issuing supervisory opinions, we provide early, practical guidance, help prevent risks to individuals' rights and freedoms, and promote a consistent application of data protection principles across the EU administration.

3.1.1. Joint control in banking supervision

In 2025, our supervisory opinions addressed key governance and transparency challenges arising in the context of the supervisory and investigative activities of the European Central Bank (ECB).

In November 2025, we issued Supervisory Opinion 18/2025 following a consultation by the ECB on a draft joint controllership arrangement with national competent authorities (NCAs) in the context of the Single Supervisory Mechanism (SSM). The SSM is the EU framework for banking supervision, bringing together the ECB and national supervisory authorities in participating countries. In this setting, several authorities jointly determine how personal data is processed for supervisory purposes.

The consultation raised practical questions on how joint controllership works in practice when different legal frameworks apply. In particular, the ECB asked whether joint controllers may designate a single authority to notify personal data breaches and to carry out prior consultation on a Data Protection Impact Assessment (DPIA), and whether this would relieve the other joint controllers of their own obligations.

First, we clarified that joint controllership does not remove individual responsibilities. Where the ECB acts as a joint controller, it must notify personal data breaches to the EDPS when the conditions under the EU data protection rules applicable to EU institutions are met. This obligation applies independently of any notification duties that NCAs may have under the General Data Protection Regulation (GDPR).

Second, we confirmed that the same approach applies to prior consultation on DPIAs. If a DPIA indicates high risks and the relevant conditions are met, the ECB must consult the EDPS. A consultation carried out by an NCA with its national supervisory authority does not replace or cover the ECB's own obligation.

Third, we recommended that these responsibilities be clearly reflected in the joint controllership arrangement itself. Clear wording helps ensure legal certainty, avoids gaps in compliance, and supports effective cooperation between authorities operating under different data protection regimes.

This opinion underlines that joint controllership is a tool for cooperation, not a mechanism to shift or centralise legal responsibilities. Each controller remains accountable under the legal framework that applies to it. By clearly allocating tasks while respecting separate obligations, EUIs and national authorities can ensure effective supervision while safeguarding individuals'

rights. The findings of this opinion provide practical guidance for joint processing arrangements beyond the banking supervision context.

3.1.2. Transparency in ECB investigations

On 16 April 2025, we issued Supervisory Opinion 6/2025 following a consultation by the European Central Bank (ECB) on proposed amendments to its internal framework for reporting, investigation and disciplinary follow-up in data protection matters. The consultation also raised questions about how and when individuals should be informed when their personal data is processed in the context of internal investigations, particularly where data has not been obtained directly from the data subject.

The opinion focused on situations in which the ECB carries out a preliminary investigation and subsequently decides not to open a formal administrative inquiry. In this context, the ECB asked how to balance its duty of confidentiality with the individual's right to information, and under which conditions information may be withheld to protect the integrity of investigative procedures.

We clarified that confidentiality during investigations must remain an exception. Where personal data is processed and sharing it no longer risks an investigation, individuals should, in principle, be informed. The mere fact that data was processed in an investigative context does not automatically justify withholding information.

We also emphasised that reliance on confidentiality exceptions requires a careful, case-by-case assessment. If the ECB considers that providing information would genuinely undermine an investigation, it should explore alternative solutions before limiting transparency, such as delaying disclosure or providing partial information.

Finally, we recommended that any decision to withhold information be clearly justified and documented. The ECB must be able to demonstrate that the conditions for applying the confidentiality exception are met in the specific circumstances of each case, rather than applying a general or automatic restriction.

This opinion highlights the need to strike a careful balance between protecting the effectiveness of internal investigations and safeguarding individuals' data protection rights. Confidentiality should not be applied by default, but only where it is strictly necessary and proportionate. By adopting clear procedures and well-documented assessments, EUIs can ensure transparency while preserving the integrity of investigative processes. The guidance provided in this opinion supports a consistent and rights-respecting approach to internal investigations across EU administration.

3.2. Safeguards for international transfers

In 2025, we continued to support EUIs in ensuring that transfers of personal data to third countries take place in full compliance with EU data protection rules. Our work in this area focused on providing practical tools and legal certainty for complex transfer scenarios, while ensuring that individuals' rights remain effectively protected when data leaves the EU legal framework.

First, we adopted a Model Administrative Arrangement (AA) for transfers of personal data from EUIs to public authorities in third countries. This model is designed to help controllers put in place appropriate safeguards where transfers are based on administrative arrangements. It sets out minimum requirements to protect personal data and reflects the approach developed at EU level for transfers between public authorities. The model is adapted to the legal context of third-country public authorities and to obligations arising under their national laws.

We underlined that the use of the Model AA does not remove the need for prior authorisation. EUIs must still carry out a transfer impact

assessment to evaluate whether the safeguards can be effectively applied in the specific third country. The model must be completed in light of that assessment and of the concrete circumstances of the transfer. Only after this analysis can EUIs request our authorisation to conclude the arrangement.

Second, through Decisions 65/2025, 66/2025 and 67/2025 we authorised transfers of personal data from the European Commission to Türkiye, North Macedonia and Serbia for the implementation of the Erasmus+ and European Solidarity Corps programmes. These cases involved remote access to Commission IT systems by processors in third countries and complex contractual chains with multiple sub-processors. We confirmed that, in this context, well-designed contractual clauses can provide appropriate safeguards, ensure enforceable rights for individuals and guarantee effective legal remedies.

Our work on international transfers in 2025 demonstrates the importance of combining practical tools with rigorous case-by-case assessments. Model arrangements and contractual clauses can facilitate cooperation with third countries, but they must be supported by thorough impact assessments and clear accountability. By following this approach, EUIs can ensure continuity of EU programmes and international cooperation while maintaining a high level of protection for personal data.

3.3. Own-initiative investigations

Investigations are our primary tool for supervision and enforcement. They allow us to examine how EUIs apply EU data protection rules in practice, particularly where there are indications of serious, systemic or widespread compliance concerns ([1]). Investigations bring together legal and technical expertise and follow a structured process, including evidence gathering, inspections and preliminary assessments ([2]). Unlike complaint handling ([3]), own-initiative investigations are launched independently and may be preceded by preparatory pre-investigation work ([4]).

3.3.1. Investigations and their impact

Through our investigative activities, we aim not only to address specific compliance issues, but also to strengthen transparency, accountability and trust in the way EUIs process personal data.

Investigations increasingly concern complex and large-scale processing operations. They often extend over several years and may involve multiple EUIs. In 2025, the growing volume of personal data processed by EUIs, combined with increasingly sophisticated technical systems and procedures, continued to lengthen investigations and raise their complexity.

([1]) In that sense, investigations are different from data protection audits, which are a regular supervisory activity of the EDPS carried out following an annual audit plan and a specific methodology to select audit targets among all EUIs.

([2]) A preliminary assessment issued by the EDPS is a procedural step in EDPS investigations and complaints proceedings similar to a draft decision issued by a national DPA or a statement of objections issued by the European Commission.

([3]) For further details on the EDPS's handling of complaints, please refer to the dedicated section on complaints (see 3.5. Complaints handling)

([4]) Before launching a formal investigation, a pre-investigation may be conducted to gather facts and to evaluate compliance and the credibility of allegations.

Effective investigations require close cooperation with national data protection authorities (DPAs). In complex cases, such cooperation is essential to assess risks consistently and to address cross-cutting technical and legal issues. At the same time, this growing need for cooperation places additional pressure on our limited supervisory resources. The investigation into the European Commission's use of Microsoft 365 is a clear example, as it required sustained expert involvement during the investigation itself, as well as during follow-up actions and related litigation.

Despite these constraints, we continued to make efficient use of available resources. In 2025, we exceeded our performance indicator for concluded enforcement activities. We adopted decisions and closed follow-up in ten investigation cases. Several of these are presented below and in the section on supervision in the AFSJ. Other investigations initiated or ongoing in 2025 will continue in 2026.

Our work does not end with the adoption of an investigation decision or audit report. We systematically monitor whether EUIs have implemented the required measures and, where appropriate, provide advice to other EUIs facing similar challenges. We also share experience with other supervisory authorities dealing with comparable issues.

The impact of our investigations therefore goes beyond formal findings or corrective measures. By prompting structural improvements and fostering a culture of compliance, investigations contribute to the broader protection of fundamental rights and to higher standards of personal data protection across EU administration.

3.3.2. Key investigation outcomes

In 2025, we continued to rely on investigations and pre-investigations as key tools to address concrete compliance risks and to promote structural improvements across EUIs. Several cases reached important milestones during the year, either through closure following corrective action, or through findings that clarified core governance requirements under EU data protection law.

We closed our pre-investigation into the European Personnel Selection Office's (EPSO) use of remotely proctored testing on 3 February 2025. This decision took into account the results of a previous EDPS audit and complaint decision, as well as the measures implemented by EPSO in response. The closure reflected progress made in addressing the identified issues, without prejudice to our ability to take further supervisory action if needed.

On 6 February 2025, we closed investigations into international transfers linked to EUIs' use of Microsoft and Amazon cloud services under Cloud II contracts. The decision was taken to ensure legal consistency while litigation concerning a related EDPS decision was ongoing, and in light of resource constraints and competing supervisory priorities. At the same time, we observed increased awareness among EUIs of their obligations regarding transfers outside the European Economic Area, including the need to better identify when transfers or remote access occur and which safeguards must be in place. These investigations may be re-opened in the future, taking into account all relevant developments.

In July 2025, we closed enforcement proceedings following our investigation into the European Commission's use of Microsoft 365. After examining the Commission's implementation of additional contractual, technical and organisational measures, we concluded that the infringements identified in our decision of March 2024 had been remedied. Improvements included clearer definition of

processing purposes, tighter control of international transfers, and stronger safeguards governing disclosures. The Commission's revised contractual arrangements are available to other EUIs, and we encouraged institutions using Microsoft 365 to carry out comparable assessments and to implement similar measures. We also provided targeted advice to EUIs in both September and December 2025 to support a common and secure baseline for the use of these services.

In 2025, we concluded investigations into the dismissal of DPOs at the Committee of the Regions and the European Defence Agency. In both cases, we found breaches of the requirement to obtain our prior consent before dismissing a DPO. These decisions reaffirmed that DPO independence is a cornerstone of effective data protection governance within EU administration. While we issued reprimands in both cases, we also took into account mitigating factors, including acknowledgment of responsibility and corrective action by the institutions concerned.

Finally, on 25 July 2025, we closed a pre-investigation into the selection of trainees for the European Commission's Blue Book Traineeship programme. Our assessment focused on whether the selection process relied solely on automated decision-making and whether adequate safeguards and transparency measures were in place. The closure was without prejudice to further supervisory action, and we subsequently decided to launch an audit at the Commission's Traineeship Office.

These cases illustrate how investigations and pre-investigations contribute to compliance beyond individual outcomes. By addressing concrete risks, clarifying governance obligations and encouraging corrective action, our investigative work strengthens data protection practices across EUIs and supports a consistent and rights-respecting approach to the processing of personal data.

3.4. Data protection audits

Data protection audits are a core supervisory tool that allows us to assess how EUIs apply data protection rules in practice.

3.4.1. Audits and their impact

Audits provide an in-depth understanding of specific processing operations and enable us to verify whether personal data is processed lawfully, securely and in line with applicable requirements, such as the principles of accountability and data protection by design obligations. They apply equally to all EUIs and contribute to fairness, legal certainty and consistency in supervision.

Audits allow us to tailor our supervisory recommendations to the concrete context of each EUI. By examining processing operations in detail, we gain insight into how an EUI acts as a controller and how data protection requirements interact with its operational needs. This enables us to issue targeted and practical recommendations, rather than abstract or generic compliance advice.

Audits also play an important preventive role. They help identify weaknesses, maladjusted practices or potential infringements at an early stage, before risks to individuals' rights and freedoms materialise or escalate. Early intervention supports EUIs in steering their processing operations towards compliance and strengthens internal governance structures.

For EUI management and DPOs, audit findings offer authoritative, independent confirmation of how key processing operations perform against legal requirements. This reassurance supports informed decision-making and reinforces accountability within the organisation.

Beyond individual findings, data protection audits contribute to transparency and trust. Independent supervision reassures staff, EU citizens and other individuals that personal data is handled responsibly and in accordance with EU law. By combining assessment,

guidance and prevention, audits remain a central element of our supervisory approach and a key driver of sustainable compliance across EU administration.

3.4.2. Key audit outcomes

In 2025, we continued to rely on data protection audits as a central supervisory tool to assess how EUIs apply data protection rules in practice. During the year, we issued audit reports and closed follow-up in sixteen audits, carried out five new on-the-spot audit activities, and pursued additional ongoing audit work. These activities enabled us to identify risks, verify compliance, and support EUIs in strengthening their internal data protection governance.

A first group of audits focused on the processing of health and medical data, where particularly high standards of protection are required. In February 2025, we issued an audit report on the Medical Service of Europol. The audit identified gaps relating to transparency, record-keeping, storage limitation, accountability, the handling of data subject requests, and the implementation of technical and organisational measures.

Similar issues were identified in audits of the European Parliament's Medical Service and of the HUMAINT (Human Behaviour and Machine Intelligence) research project at the Commission's Joint Research Centre, including shortcomings in retention practices, the lawfulness of processing sensitive data and security safeguards. Our recommendations aimed to establish clearer rules, improve documentation and reinforce protective measures, particularly where vulnerable individuals or sensitive data is concerned.

A second set of audits addressed large-scale and innovative processing operations. In January 2025, we issued an audit report on the European Centre for Disease Prevention and Control which focused on the use of data from the GISAID (Global Initiative on Sharing All Influenza Data) platform, social media monitoring for epidemic intelligence, restrictions of data subject rights, and access controls for surveillance systems.

In November 2025, we also issued an audit report on the European Commission's EU Login mobile application, following up on our guidance on mobile applications. In both cases, we issued recommendations to strengthen transparency, retention practices, information security, record-keeping, and the clear allocation of data protection responsibilities.

Finally, in September 2025, we closed follow-up on audits of twenty-one EUI websites carried out in previous years. This work focused on the implementation of recommendations concerning website security, the use of cookies or similar technologies, and respect for browser signals such as 'Do Not Track'. While not all aspects were re-checked, we emphasised the responsibility of EUIs to fully implement and document all outstanding recommendations in line with the accountability principle.

In addition to completed audits, we carried out on-the-spot checks at the Commission's Traineeship Office, the European Labour Authority's EURES (European Employment Services) system, and the Customs Information System, and continued follow-up on earlier audits.

All ongoing audit work will continue in 2026. Taken together, these activities show how audits contribute not only to individual compliance outcomes, but also to sustained improvements in data protection practices, accountability and trust across the EU administration.

3.5. Complaints handling

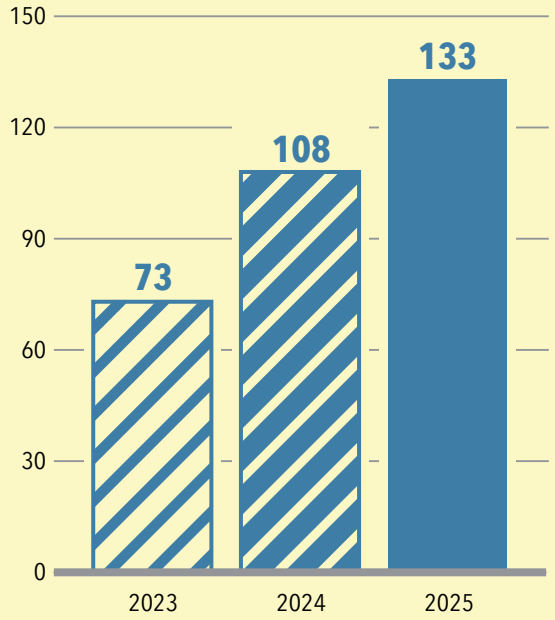
Handling complaints from individuals is a central element of our supervisory mandate. Complaints allow individuals to challenge how EUIs process their personal data and provide us with direct insight into areas where data protection rules may not be applied effectively in practice. In recent years, both the number

and the complexity of admissible complaints have continued to increase, reflecting greater awareness of data protection rights and more complex processing environments within EU administration.

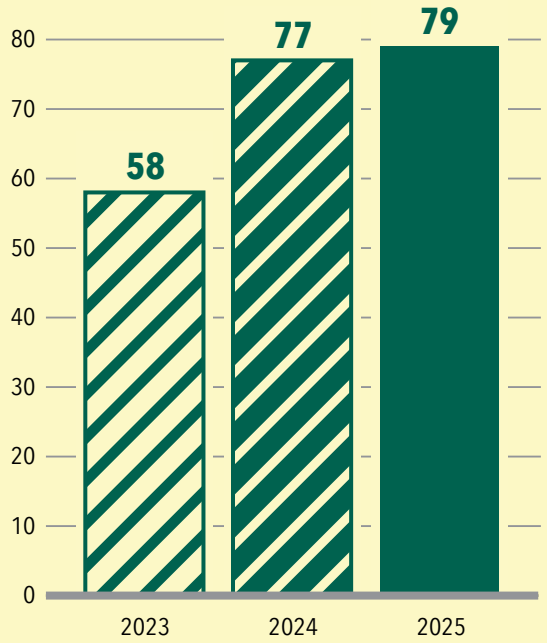
3.5.1. Complaint handling and statistics

In 2025, we received 133 admissible complaints, representing an increase of 23% compared to 2024. By the end of the year, 180 admissible complaints were ongoing, including cases submitted in previous years. The time required to handle a complaint depends on several factors, including the complexity of the processing at issue, the need for technical assessments, and interactions with the EUI concerned ([5]). Despite these challenges, we exceeded our performance indicator for concluded enforcement activities and issued decisions and closed follow-up in 79 admissible complaint cases in 2025 ([6]).

Graph 1
Admissible complaints received



Graph 2
Concluded admissible complaints



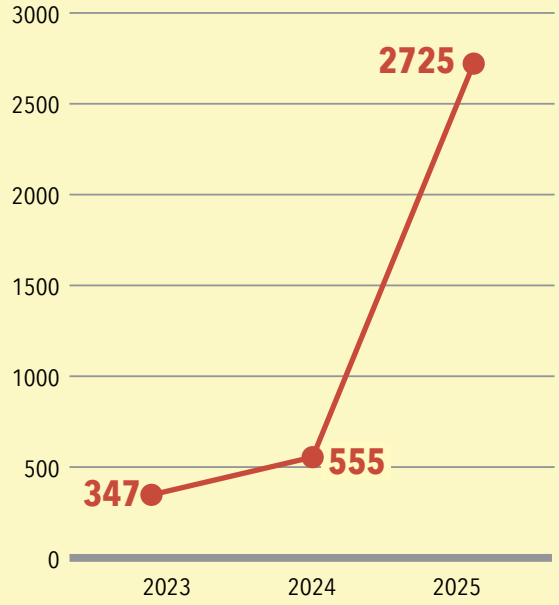
([5]) These factors are: the complexity of the subject matter; the need to obtain the views of the parties to the case and other involved entities entails multiple exchanges where the responsiveness of the controller/complainant/other entity is beyond the EDPS's control; whether there are any other complaints on the same or similar subject matter against the same or another EUI; the need to obtain any further information to assess potential rule-breaking; the need for on-the-spot checks or remote investigations of the complaint; any concurrent or planned EDPS enforcement actions on the same or similar matters; the need for any suspension of handling and investigating a complaint because of a pending case before courts or administrative bodies; EDPS resource constraints.

([6]) A complaint procedure can be concluded either by: referral to the data protection officer of the EUI; referral to a controller in the EUI; amicable settlement or other resolution during the investigation phase; formal decision of the EDPS; or pursuit of the matter through other EDPS enforcement actions (such as an audit or own-initiative investigation). After issuing a decision in a complaint case, the EDPS systematically checks how the EUIs concerned implement corrective measures imposed by the EDPS in its decision.

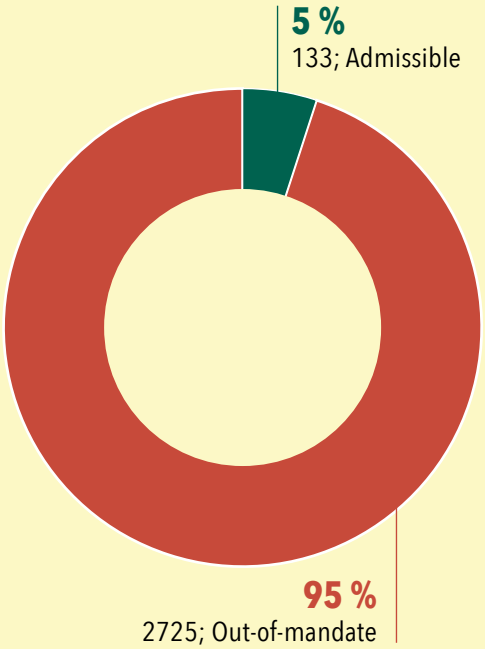
There was a significant rise observed in complaints that fall outside our mandate, which are considered inadmissible from the outset. In addition to admissible complaints, we received 2,725 inadmissible or out-of-mandate complaints in 2025, compared to 555 in 2024 – an increase of almost 500%. These out-of-mandate complaints typically concern processing carried out by private entities, national authorities or international organisations, which do not fall within our competence. The sharp increase is linked to the growing use of automated and AI-based tools that may misdirect individuals to submit complaints to the EDPS that do not come under our jurisdiction.

While we cannot take enforcement action on out-of-mandate complaints, we responded to all such submissions. In 2025, we further streamlined our response procedures and strengthened public information on the scope of our mandate, with the aim of guiding individuals more effectively towards the competent authority when the EDPS is not empowered to act.

Graph 4
Out-of-mandate complaints (2023–2025)



Graph 3
Admissible v. out-of-mandate complaints



Admissible complaints most frequently concerned individuals' rights, in particular the right of access to personal data and the right to be informed about processing activities. Security and confidentiality of processing were also commonly raised. As in previous years, the majority of admissible complaints were submitted by staff members of EUIs, and most complaints concerned the European Commission, reflecting its size, role and range of activities.

Our complaints-handling work in 2025 highlights both the growing demand for effective redress mechanisms and the importance of clear communication about supervisory competences. By resolving admissible complaints, responding to out-of-mandate submissions and identifying recurring issues, we contribute to strengthening individuals' rights, improving compliance by EUIs and reinforcing trust in data protection supervision across EU administration.

3.5.2. Key complaint decisions

A number of decisions issued in 2025 illustrate how complaints handling contributes to clarifying key data protection principles in practice.

In March 2025, we issued a decision concerning the transmission of EU staff members' personal data to the Permanent Representations of Member States. The complaint related to the regular transmission by an EUI of multiple categories of staff data, including contact details, employment information and nationality. We found that only a limited set of data – namely names, grades and addresses – may be transmitted on the basis of the relevant EU rules establishing privileges and immunities. ([7]) As the EUI could not demonstrate a valid legal basis for transmitting additional categories of personal data, we concluded that the processing infringed the principles of lawfulness, data minimisation and purpose limitation. We issued a reprimand and ordered the EUI to stop transmitting data beyond what is strictly required. Given the broader relevance of this issue, we also provided guidance to all EUIs on how to assess and limit such transmissions.

Another decision issued in April 2025 concerned data protection by design and by default ([8]) in the context of the European Commission's EU Funding and Tenders Portal. Following a complaint against the Commission's Directorate-General for Informatics, we assessed the procedure for activating a Legal Entity Appointed Representative (LEAR) account. We concluded that appropriate technical and organisational measures were in place to ensure secure authentication and to limit access to personal data to authorised persons only. We also found that internal instructions were clear, regularly reviewed and adequate to ensure the security of the processing.

([7]) Based on Article 15(2) of Protocol No 7 to the TFEU.

([8]) See also EDPS Preliminary Opinion on Privacy by Design and EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

In June 2025, we addressed a complaint against the EPSO concerning access to handwritten notes of a selection board. We balanced the complainant's right of access with the need to protect the confidentiality and impartiality of selection procedures and the rights of others. We concluded that these interests could be reconciled by providing a joint typed summary of the notes, with a level of detail that safeguards the secrecy of the proceedings while allowing the individual to exercise their right of access.

Finally, in December 2025, we issued a decision on an unlawful disclosure of email addresses following a request for public access to documents. We found that the disclosure was not necessary and that several core data protection principles had been infringed. While the EUI concerned implemented corrective technical and organisational measures during the proceedings, we issued a reprimand to underline the importance of carefully assessing the necessity of disclosing personal data in response to access to documents requests.

3.6. Court cases and litigation

Judicial proceedings form an important part of our mandate. We may bring cases before the Court of Justice of the European Union (CJEU) and the General Court, defend our decisions when they are challenged, or intervene in proceedings that raise issues of relevance for data protection supervision. Through litigation, we contribute to the interpretation and development of EU data protection law and ensure that fundamental rights are effectively protected at EU level.

In 2025, several court cases addressed core questions relating to transparency, the notion of personal data and the limits of international data transfers. Some of the most significant developments are outlined below.

A landmark judgment was delivered on 4 September 2025 by the CJEU in the case *EDPS v Single Resolution Board* (C-413/23 P). The Court set aside the General Court's judgment.

The case concerned the transfer by the Single Resolution Board (SRB) of pseudonymised comments from individuals to an external consultancy without informing the data subjects. The Court confirmed, in particular, that personal opinions are inherently linked to individuals, that pseudonymised data may not necessarily constitute personal data from the recipient's perspective (if they are unable to re-identify individuals), and that the obligation to inform data subjects applies at the moment personal data is collected.

The judgment reaffirmed our interpretation of the right to information and has broader implications for supervisory practice. Following the ruling and the referral of the case back to the General Court, the SRB discontinued the proceedings, and the case was removed from the register in December 2025.

In 2025, proceedings were also ongoing in the appeal case EDPS v Parliament and Council (C-698/23 P). The appeal concerned the EDPS's standing to bring an action for annulment against two provisions of the amended Europol Regulation which, in the view of the EDPS, affected personal data processing operations carried out by Europol, undermining legal certainty for individuals and interfering with the independence of the EDPS.

In May 2025, Advocate General Campos Sánchez-Bordona delivered an opinion concluding that the EDPS has the legal right to bring the action for annulment, as the contested provisions directly and individually concern the EDPS.

The judgment in this case is expected to provide further clarification on the role of the EDPS as an independent data protection supervisory authority at EU level, particularly regarding its ability to seek judicial review of legislative provisions that directly affect personal data processing operations and the effective exercise of its supervisory mandate.

In addition, on 28 July 2025, the European Commission and Microsoft Ireland Operations discontinued their actions against our decision of 8 March 2024 concerning the Commission's use of Microsoft 365. As a result, the General Court removed the joined cases T-262/24 and T-265/24 from its register in September 2025. These developments confirmed the relevance of our supervisory findings while bringing procedural closure to the litigation.

Court proceedings in 2025 played a significant role in clarifying key data protection concepts and reinforcing supervisory principles. Through strategic litigation and defence of our decisions, we contribute to legal certainty for EUIs and to the consistent protection of individuals' rights across the EU legal order.

3.7. DPO network and DPO-related matters

The DPO network is a cornerstone of our engagement with EUIs. It provides a structured forum for dialogue, mutual learning and coordination, and supports the consistent application of data protection rules across the EU administration. Through the network, we gain direct insight into the practical challenges faced by DPOs and can tailor our supervisory guidance accordingly.

In 2025, our work with the DPO network focused on strengthening the role and independence of DPOs, supporting them in addressing emerging technological and organisational challenges and fostering a shared understanding of good practice.

We also contribute to strengthening the independence of DPOs by intervening in individual cases concerning their dismissal before the expiry of their term of designation.

3.7.1. Key activities

In 2025, we held two EDPS-DPO meetings, marking the 56th and 57th sessions of the network. These biannual meetings bring together DPOs from across EU administration and remain a key forum for exchanging experience

and discussing topical data protection issues. Discussions in 2025 addressed, in particular, the impact of emerging technologies, the prevention of personal data breaches, website compliance, and recent supervisory developments as regards DPOs, including on their independence and on avoidance of conflicts of interest. The outcomes of this activity were reflected in the EDPS's new supervisory guidance on the role of DPOs in EUIs.

The network operates on a collaborative basis, with each meeting hosted in turn by the DPO of an EUI. This approach reinforces peer-to-peer engagement and shared ownership of the network. The meetings were supported by the DPO Support Group, a rotating group of volunteer DPOs who worked closely with us to shape agendas and prepare interactive sessions, such as workshops and case studies.

Beyond plenary meetings, we continued to support DPO roundtables, which bring together smaller groups of DPOs for focused exchanges on specific topics. In 2025, these discussions addressed issues such as the right to erasure, storage limitation, DPO independence and the handling of manifestly unfounded or abusive requests. Participation was managed to ensure balanced representation across EUIs.

We also adopted decisions in individual cases concerning the dismissal of DPOs, reaffirming that prior consent from the EDPS is required and that DPO independence is a fundamental element of effective data protection governance.

Our engagement with the DPO network in 2025 illustrates its value as both a support mechanism and a supervisory interface. By combining dialogue, guidance and targeted intervention, we strengthen the role of DPOs and promote a consistent, practical and rights-respecting application of data protection rules across EU administration.

3.8. Surveys

Surveys are an important tool for our general monitoring activities. They allow us to assess, in a structured and comparable way, how EU institutions, bodies, offices and agencies (EUIs) apply EU data protection rules in practice and to identify common trends, challenges and areas for improvement.

In September 2025, we published a report on a survey examining how EUIs conduct DPIAs. The survey aimed to assess current practices and to compare them with the findings of our 2020 survey, taking into account the increased experience EUIs have gained in carrying out DPIAs since then.

Given the volume and complexity of the responses, we focused on identifying overarching trends and significant outliers rather than providing individual feedback to each EUI. This approach enabled a robust analysis of collective practices and highlighted both areas of convergence and instances where further attention is needed.

The results show progress in the understanding and use of DPIAs across EU administration, while also pointing to remaining challenges in the depth of risk analysis, the description of mitigation measures and the integration of DPIAs into decision-making processes. The insights gained from this survey will directly inform updates to our guidance on DPIAs and support EUIs in strengthening their risk assessment practices.

By combining monitoring with targeted follow-up, surveys help us promote a more consistent and effective application of data protection requirements. The 2025 DPIA survey provides a valuable evidence base for refining supervisory guidance and supporting EUIs in embedding data protection by design and by default in their processing operations.

3.9. Supervision of the Area of Freedom, Security and Justice

As part of our mandate, we supervise the processing of personal data by EUIs operating in the Area of Freedom, Security and Justice (AFSJ). This includes:

- the European Union Agency for Law Enforcement Cooperation (Europol);
- the European Union Agency for Criminal Justice Cooperation (Eurojust);
- the European Public Prosecutor's Office (EPPO);
- the European Border and Coast Guard Agency (Frontex);
- the European Union Agency for Asylum (EUAA);
- the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA);
- the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).

Together, these bodies operate across a broad range of policy areas, including border management, asylum and immigration, police cooperation, the fight against serious crime, and judicial cooperation in civil and criminal matters.

The AFSJ is characterised by extensive and often sensitive processing of personal data, frequently involving individuals in vulnerable situations and operations with significant implications for fundamental rights.

Building on the experience gained under the 2020-2024 Strategy, we continued in 2025 to address the structural challenges arising from a fragmented legal and operational framework governing police and judicial cooperation and border management. In a context marked by evolving operational practices and increasing technological complexity, our supervisory approach focused on ensuring the consistent and effective application of EU data protection law, in particular Regulation (EU) 2018/1725 and its Chapter IX.

In 2025, our supervisory activities in the AFSJ were structured around seven interrelated priority pillars, covering:

- preparation for the interoperability framework;
- supervision of the interoperability framework;
- ex ante and ex post supervision of Europol's operational and technological developments;
- oversight of large-scale processing of personal data at the EU's external borders, in particular by Frontex;
- supervision of new and evolving processing operations at Eurojust and the European Public Prosecutor's Office;
- scrutiny of the use of artificial intelligence and other innovative technologies in law enforcement and border management;
- coordinated supervision and close cooperation with national DPAs.

Together, these pillars supported a proportionate, risk-based and coherent supervisory approach across the EU administration in a highly sensitive operational environment.

3.9.1. Preparing for and supervising the interoperability framework

The EU is progressively establishing an interoperability framework to enable the exchange of information between large-scale EU information systems in the areas of borders, visa policy, migration, asylum, police cooperation and judicial cooperation. This framework brings together existing systems, such as the Schengen Information System, the Visa Information System and Eurodac (European Asylum Dactyloscopy Database), alongside new systems, including the Entry/Exit System, the European Travel Information and Authorisation System (ETIAS) and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).

The interoperability framework introduces a shared technical and operational architecture allowing data stored in different systems to be interconnected, combined and queried, including through advanced biometric identification techniques and risk-screening algorithms. As the framework gradually enters into operation, with full deployment foreseen by 2028, it raises significant challenges for data protection oversight, given the scale of the data involved, the sensitivity of the processing and the potential impact on individuals' fundamental rights.

In 2025, we continued to prepare our supervision of the interoperability framework. Our activities focused on monitoring the development of ETIAS, providing guidance on the progressive start of the Entry/Exit System, and strengthening cooperation with national DPAs to ensure coherent oversight across the EU.

Supervisory opinion on the ETIAS watchlist

In March 2025, we issued Supervisory Opinion 2/2025 to Europol concerning its implementation of the ETIAS watchlist. ETIAS is designed to pre-screen travellers from visa-exempt countries before their arrival at the EU's external borders, enabling authorities to assess risks related to irregular migration, security and public health.

The ETIAS Regulation provides for the establishment of a watchlist containing data on individuals suspected of having committed, or of being likely to commit, terrorist or other serious criminal offences. Both Europol and Member States contribute data to the watchlist and remain responsible for the data they enter.

In our opinion, we assessed Europol's draft Management Board Decision setting out the procedures governing its responsibilities in entering data into the watchlist. We issued a number of recommendations aimed at ensuring compliance with data protection rules. In particular, we emphasised the need for clear, detailed and well-documented criteria to assess whether personal data are adequate, accurate and sufficiently relevant for inclusion in the watchlist, as well as for regular review of whether the conditions for inclusion continue to be met. Such safeguards are essential to ensure that the significant interference with individuals' fundamental rights resulting from inclusion in a Europe-wide watchlist is strictly necessary and justified.

ETIAS Fundamental Rights Guidance Board

In 2025, we continued to closely follow the development of ETIAS through our active

participation in the ETIAS Fundamental Rights Guidance Board. This body, established under the ETIAS Regulation, provides independent guidance on the fundamental rights implications of the processing of ETIAS applications.

Five formal meetings of the Guidance Board took place in 2025, alongside expert working group meetings involving national authorities and EU agencies to coordinate specific aspects of ETIAS implementation. In March 2025, the Guidance Board issued a guidance note on fundamental rights considerations when informing ETIAS applicants, with a particular focus on ensuring the right to an effective remedy and to a fair trial.

The Guidance Board was also consulted during the development of the ETIAS analytical framework for the screening rules. In this context, it provided substantive input on methodological documents and contributed to discussions on the design of the risk-screening operations underpinning the algorithmic profiling used in ETIAS. Throughout 2025, the Board continued to monitor how data protection by design is integrated into the development of ETIAS, including issues related to the Data Protection Impact Assessment, controllership arrangements and the processing of law enforcement data.

Guidance on the progressive start of the Entry/Exit System

The Entry/Exit System (EES) is a new EU-wide digital border management system that replaces manual passport stamping with the automated recording of biographic and biometric data of non-EU nationals entering and leaving the Schengen area for short stays. In 2025, the EU adopted a temporary derogation allowing for a progressive rollout of the system rather than a simultaneous start in all Member States. Under this approach, operations began on 12 October 2025 and are being introduced gradually over a six-month period.

In June 2025, we issued joint comments with the European Data Protection Board's Coordinated Supervision Committee (see section 3.9.6. Coordinated supervision and cooperation with national data protection authorities below) on the European Commission's information campaign materials relating to the progressive start of the system. We recommended that the materials be revised to ensure that non-EU nationals receive clear, precise and scenario-specific information about which data are collected, for what purposes and with what consequences, in line with transparency requirements. We also identified broader shortcomings, including insufficient information on data access by authorities, the objectives of the system and the practical exercise of data subject rights. These comments were made in light of the Commission's failure to consult supervisory authorities as required by the Entry/Exit System Regulation.

In September 2025, we also responded to a consultation on draft practical guidance developed by the Commission for national authorities during the progressive rollout. Our recommendations focused on mitigating risks arising from potentially incomplete or inaccurate data during this period. In particular, we addressed the reliability of automated calculation tools, the risks linked to access by other authorities and systems, and the handling of requests to correct or complete data.

3.9.2. Europol

In 2025, we continued to supervise the personal data processing activities of the European Union Agency for Law Enforcement Cooperation (Europol), with particular attention to high-risk processing operations. Our supervisory focus reflected Europol's expanding mandate, the increasing scale and complexity of the data it processes, and the growing

reliance on advanced technologies. Priority areas included the use of artificial intelligence and machine-learning tools, Europol's access to EU large-scale IT systems, the use of information from publicly available sources, new forms of data collection, joint operational environments, and cooperation with third countries and private parties.

To address these developments, our supervisory activities combined ex ante oversight, inspections and follow-up, cooperation with national DPAs, and engagement with democratic oversight bodies.

Ex ante supervision of Europol's operational and technological developments

In 2025, we issued eight supervisory opinions following requests for prior consultation by Europol concerning new or significantly modified processing operations. One request was withdrawn before an opinion was adopted. These consultations covered a wide range of high-risk developments.

A significant part of our work concerned the increasing use of machine learning and artificial intelligence. Europol processes very large and complex datasets originating from multiple sources, including seized digital devices. To support operational analysis, Europol consulted us on the development of new machine-learning models for its 'Machine Learning Toolbox' and on the use of existing models to categorise uncategorised personal data.

In our opinions, we assessed both the lawfulness of developing these models and their subsequent use. We clarified the applicable legal bases depending on whether operational or open-source personal data are used, and confirmed that the specific regime introduced by the 2022 amendment of the Europol Regulation applies to the processing of data that has not yet been fully categorised. We also examined the proportionality and necessity of these processing operations.

Europol also consulted us on a tool designed to detect faces in images and videos and to automatically blur those of minors. Given unresolved questions regarding the applicable legal framework for fine-tuning machine-learning models using open-source data, Europol decided to pause the consultation and to resubmit it at a later stage based on an updated impact assessment.

Another priority area concerned Europol's access to EU large-scale IT systems (LSITs). We assessed proposed processes for querying the Entry/Exit System and issued recommendations to ensure that searches are limited to eligible categories of individuals, that proportionality assessments are properly documented, and that matches are subject to meaningful human review. We also advised Europol on procedures for entering information alerts in the Schengen Information System based on data received from third countries, with a focus on avoiding inconsistent or disproportionate use and clarifying responsibilities between systems. In addition, we examined Europol's proposed use of fingerprints to query the Visa Information System and identified safeguards to mitigate the risks associated with unnecessary biometric searches.

We also addressed new forms of data collection, including a proposed cyber threat intelligence platform and a tool for retrieving and analysing publicly available block chain data. In these cases, we clarified the conditions under which publicly available information may be processed and required Europol to rely on the specific legal regime applicable to uncategorised data, including strict necessity, proportionality and short retention periods.

Finally, we issued recommendations on new analytical tools and environments, including systems used to analyse material related to child sexual abuse and a proposed Internet-facing operational environment. Our advice focused on limiting data intake, restricting retention periods and ensuring adequate oversight mechanisms.

Building on clarifications provided in earlier opinions, we continued in 2025 to advise Europol on issues arising from joint operational analysis with Member States. We reiterated that such processing qualifies as joint controllership and requires a detailed Joint Controllership Arrangement setting out responsibilities towards data subjects and supervisory authorities. We clarified that arrangements must cover, in particular, transparency obligations, the handling of access requests, cooperation in impact assessments and prior consultations. While such arrangements allocate responsibilities, each joint controller remains subject to its own legal framework and supervision by its competent authority, including the obligation to consult its respective supervisory authority where required.

Europol Innovation Lab

Following amendments to the Europol Regulation, Europol is now authorised to carry out research and innovation projects under a dedicated legal regime. In 2025, we received the first notifications relating to projects launched within the Europol Innovation Lab. This prompted supervisory work to clarify the scope of "operational personal data" and the definition of research and innovation projects. Our assessment of these projects is ongoing.

Audits and inspections

In July 2025, we carried out an inspection at Europol in cooperation with experts from national DPAs. The inspection focused on Europol's use of the Schengen Information System, facial recognition solutions, transfers to third countries and international organisations, and exchanges of data with private parties. The scope was defined on the basis of identified risks, recent developments and previous supervisory findings.

We also decided to close follow-up on inspections carried out between 2017 and 2019, taking into account Europol's high implementation rate of previous recommendations and the extensive supervisory dialogue that had taken place. Responsibility for the remaining actions lies with Europol under the accountability principle.

Joint Parliamentary Scrutiny Group (JPSG) on Europol

In 2025, the Supervisor participated in both meetings of the Joint Parliamentary Scrutiny Group on Europol. In February, discussions focused on joint operational analysis and the use of artificial intelligence in law enforcement, highlighting the need for clear allocation of responsibilities and cautious use of high-risk technologies. In November, the Supervisor shared lessons learned from supervisory experience, emphasising the importance of strong ex ante supervision, prior consultations and impact assessments. As Europol's mandate continues to expand, proactive and coordinated data protection supervision remains essential to safeguard fundamental rights, ensure accountability and support lawful law enforcement cooperation.

3.9.3. Processing of personal data at EU borders

The processing of personal data at the EU's external borders raises particular data protection challenges, given the scale and sensitivity of the operations involved and the frequent impact on individuals in vulnerable situations. In 2025, our supervision in this area focused primarily on the activities of the European Border and Coast Guard Agency (Frontex), combining investigation, audit follow-up and operational engagement to ensure that personal data are processed fairly, lawfully and with appropriate safeguards.

Formal investigation: Frontex's collection of individuals' personal data at EU external borders

In 2025, we continued a formal investigation into Frontex's collection of personal data during debriefing interviews conducted with individuals intercepted at the EU's external borders. This investigation builds on findings from our 2022 audit, which raised serious concerns regarding compliance with the principle of fairness and the allocation of data protection responsibilities for the processing of information collected during these interviews.

The concerns identified in the audit were subsequently confirmed and further substantiated during a pre-investigation carried out in 2023, including an on-site inspection in Lesvos. In light of these findings, and taking into account Frontex's delayed or incomplete implementation of the 2022 audit recommendations, we decided in 2024 to open a formal investigation into suspected infringements of Regulation (EU) 2018/1725.

During 2025, we continued to gather and analyse relevant evidence. On that basis, we concluded the investigative phase and prepared a preliminary assessment setting out established facts, an initial legal assessment and the suspected infringements. This preliminary assessment was communicated to Frontex, which was invited to submit its observations.

Operational visit on returns

Third-country nationals without a legal right to stay in the EU have to return to their country of origin. In this context, Frontex may provide operational and technical support to a requesting EU country at different stages of the return process. On 30 September 2025, we carried out an operational visit to Frontex's headquarters in Warsaw to deepen our understanding of return-related procedures and the data protection safeguards applied in practice. The visit focused on how personal data is processed in the context of return operations and reintegration assistance.

Returns were selected as a priority area in view of Frontex's expanding role, reflected in the increasing number of assisted and organised returns and the intensification of reintegration activities. The visit also took place against the background of potential future changes to Frontex's mandate under the proposed Returns Regulation and the planned revision of the European Border and Coast Guard Regulation.

The visit strengthened our understanding of Frontex's operational role and data processing practices in this area and helped inform our future supervisory activities, including potential consultations, investigations or audits related to return operations.

Audit of Frontex: close monitoring of follow-up and closure of the pending recommendations

In 2025, we continued to closely monitor the implementation of recommendations stemming from the audit carried out at Frontex's headquarters in October 2022. That audit

examined Frontex's activities at EU borders during joint operations, with a particular focus on interviews of individuals crossing borders without authorisation and the subsequent processing of personal data.

The audit resulted in 32 recommendations addressing identified shortcomings. By May 2025, five recommendations remained pending, while ten were being addressed in the context of the ongoing formal investigation. The remaining issues related in particular to the collection of personal data on suspected cross-border crimes, the transmission of such data to Europol, and the completion of data protection impact and security risk assessments.

On 28 November 2025, we decided to close the audit follow-up, taking into account that Frontex had adopted specific rules governing the collection of operational personal data and their transmission to Europol. We also noted the implementation of several security controls identified as necessary to mitigate data protection risks. At the same time, we emphasised that, in line with the accountability principle, Frontex remains responsible for completing the implementation of the remaining security measures.

3.9.4. Eurojust

In the AFSJ, we are responsible for supervising the processing of operational personal data by Eurojust. Our supervision aims to ensure that Eurojust's activities comply with the applicable EU data protection framework, in particular Regulation (EU) 2018/1727, as well as other relevant provisions of EU law. In 2025, our work focused on Eurojust's expanding mandate in relation to core international crimes and on new tasks linked to criminal records information concerning third-country nationals.

Core International Crimes Evidence Database

Following the entry into force of the amended Eurojust Regulation (Regulation (EU) 2022/838), Eurojust was given an explicit legal basis to preserve, store and analyse evidence related to genocide, crimes against humanity, war crimes and related criminal offences. This measure was introduced in response to the Russian aggression against Ukraine, with the aim of securing storage of evidence outside Ukraine and supporting investigations and prosecutions by European and international judicial authorities. To support these tasks, Eurojust developed the Core International Crimes Evidence Database (CICED). Since 2022, we have closely accompanied the development of CICED to ensure that its design and operation comply with Union data protection rules.

Prior to 2025, we had already issued four supervisory opinions on CICED, addressing the secure transmission and storage of evidence, the analysis of structured data and the use of automated translation tools. In 2025, we issued a further supervisory opinion following a fifth prior consultation, which concerned the introduction of an optical character recognition tool and new arrangements for sharing CICED data with internal and external stakeholders. In this opinion, we issued recommendations aimed at mitigating the additional risks introduced by these new processing operations.

In addition, in 2025 we issued our audit report following an on-site audit carried out in June 2024. The audit examined Eurojust's compliance with the applicable data protection rules when processing operational personal data in CICED and with our earlier supervisory recommendations. The report contained 31 recommendations. During the follow-up phase, we observed significant progress and noted that more than half of the recommendations had already been implemented.

Given that CICED processes highly sensitive crime-related data concerning different categories of data subjects, including victims, suspects and witnesses, additional safeguards apply under the legal framework. In May 2025, we therefore carried out a targeted audit at Eurojust's premises to verify compliance with the specific requirements applicable to the processing of special and other sensitive categories of data within CICED.

European Criminal Records Information System – Third Country Nationals

In 2025, we were consulted and issued a supervisory opinion on a number of legal issues relating to Eurojust's tasks under the Regulation on ECRIS-TCN. This centralised system enables Member State authorities to determine efficiently which Member State or States hold criminal record information on a third-country national.

Under this framework, Eurojust receives requests from third countries for the purpose of identifying whether criminal record information on a third-country national is held by a Member State. Our opinion focused on ensuring consistency between this newly introduced task and the existing provisions of the Eurojust Regulation.

We concluded that, given Eurojust's limited role as a contact point and the fact that decision-making powers and effective control remain with the Member States, Eurojust should be regarded as acting as a processor for this processing operation, while the Member States act as controllers. We also assessed the technical means used for processing the operational personal data received in this context and provided guidance to ensure that appropriate safeguards are applied.

EUROPEAN PUBLIC PROSECUTOR'S OFFICE

3.9.5. European Public Prosecutor's Office

The EPPO was established by Regulation (EU) 2017/1939 to investigate, prosecute and bring to justice criminal offences affecting the EU's financial interests, including fraud, corruption and serious cross-border VAT fraud. To fulfil this mandate, the EPPO processes operational personal data in highly sensitive law enforcement contexts and is subject to supervision by the European Data Protection Supervisor.

Audit follow-up and supervisory outcomes

In 2023, we carried out an audit at the EPPO's premises to assess its compliance with EU data protection law and with the EPPO Regulation when processing operational personal data. The audit focused in particular on the handling of individuals' access requests and on the use of the Case Analysis Tool Environment (CATE), a system used to analyse personal data, on which we had also issued a separate supervisory opinion.

The audit report identified eleven formal findings and included five recommendations aimed at strengthening the protection of individuals' rights and improving governance and storage practices within CATE. In 2024, we observed progress in the implementation of these recommendations and closed three of them.

In 2025, we continued to monitor the remaining two recommendations. During this follow-up phase, we decided to close both recommendations. At the same time, we noted that one recommendation had not been implemented by the EPPO, which may give rise to non-compliance with the relevant provisions of the

EPPO Regulation. This conclusion underlines the importance of continued vigilance and accountability in the processing of operational personal data in the context of criminal investigations.

Our supervisory work on the EPPO in 2025 demonstrates the role of audits and follow-up as tools to support compliance over time. By monitoring the implementation of recommendations and assessing residual risks, we contribute to ensuring that the EPPO's operational effectiveness is accompanied by a high level of data protection and respect for individuals' fundamental rights.

3.9.6. Coordinated supervision and cooperation with national data protection authorities

Coordinated supervision with national DPAs is essential to ensuring effective and consistent oversight of LSITs and EUIs operating in the AFSJ. Given the shared responsibilities between EU and national authorities in this field, close cooperation is necessary to address cross-border processing operations, clarify governance arrangements and safeguard individuals' rights.

In 2025, our work in this area focused on strengthening coordination mechanisms and adapting supervisory approaches to new and evolving systems.

Coordinated Supervision Committee

The European Data Protection Supervisor plays a central role in ensuring effective supervision of LSITs and Union bodies in the AFSJ through active cooperation with national supervisory authorities within the Coordinated Supervision Committee (CSC). In 2025, our work within the CSC focused on managing the expansion of its mandate, including the integration of additional systems such as the Visa Information System, and on preparing for the operationalisation of the interoperability framework.

As the CSC assumed responsibilities for new and evolving systems, we continued to promote more agile and effective working methods. As Chair of the Committee, we facilitated the establishment of dedicated working groups for the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). These structures enabled faster and more coordinated supervisory action, including the issuance of joint informal comments on the EES information campaign to improve transparency for data subjects.

We also led discussions within the CSC to clarify complex legal questions arising from joint EU–Member State processing. This included clarifying the allocation of controller and processor roles in the context of the interoperability framework and examining the status of law enforcement authorities as recipients of ETIAS data. In addition, coordinated work continued on the assessment of Europol's processing of personal data relating to minors, with particular attention to the protection of vulnerable individuals.

Eurodac Supervision Coordination Group

In 2025, we continued to participate actively in the Eurodac Supervision Coordination Group, supporting cooperation and effective oversight of the Eurodac system. Eurodac is an LSIT processing biometric data, notably fingerprints, to support EU asylum and migration policies.

With the application of the new Eurodac Regulation from June 2026, coordinated supervision of the system will be ensured within the framework of the Coordinated Supervision Committee, in accordance with Regulation (EU) 2018/1725. We will continue to work closely with national supervisory authorities to ensure a smooth transition to this new supervisory setup and to maintain a high level of data protection.

Overall, cooperation with national supervisory authorities remained a cornerstone of our approach. By working together within coordinated supervision structures, we strengthened

consistency, effectiveness and coherence in the supervision of AFSJ-related processing operations, contributing to the protection of fundamental rights and the rule of law.

3.9.7. Use of supervisory powers in the AFSJ

Throughout 2025, we exercised our supervisory powers across the AFSJ in a targeted and proportionate manner, taking into account the specific mandates, risk profiles and operational needs of each body, office and agency. Our activities included advisory actions, investigative measures and, where necessary, the use of corrective powers. These tools were applied in a complementary way to address identified risks and to promote compliance across the EU administration.

The table illustrates how the EDPS exercised its supervisory powers in the AFSJ in 2025, highlighting both the intensity and the differentiated nature of oversight across the EU administration. In total, 23 supervisory actions were carried out, with a clear emphasis on advisory measures (18), complemented by investigative actions (3) and targeted use of corrective powers (2). Europol accounted for the largest share of activity, reflecting its extensive mandate, operational complexity and high-risk data processing, while Eurojust and Frontex were subject to more focused supervisory engagement aligned with their specific risk profiles. The absence of corrective measures for most bodies indicates that supervision primarily operated ex ante and through guidance, audits and investigations, allowing risks to be addressed before enforcement became necessary. Overall, the table demonstrates a proportionate, risk-based and effective supervisory approach, combining prevention, scrutiny and enforcement to safeguard fundamental rights while supporting the lawful functioning of the EU administration in the AFSJ.

Table 2
Use of EDPS supervisory powers in the AFSJ

Body / Agency	Advisory	Investigative	Corrective	Total
Europol	10	3	2	15
Eurojust	4	-	-	4
EPPO	-	-	-	-
Frontex	2	-	-	2
eu-LISA	-	-	-	-
EUAA	-	-	-	-
European Commission	2	-	-	2
Total AFSJ	18	3	2	23

Advisory = opinions on consultations and on prior consultations, audits (carried out and reports issued), informal comments on working arrangements, operational visits

Investigative = pre-investigations (concluded), investigations (concluded), complaints (concluded or suspended)

Corrective = use of corrective powers

3.10. Guidelines on the EU Data Protection Regulation

In 2025, we adopted new and updated supervisory guidance to support EUIs in applying the EU data protection rules in a consistent and practical manner. This guidance responds to evolving technological developments, supervisory experience and feedback received from EUIs, and aims to translate legal requirements into concrete, operational recommendations.

Two guidance documents were particularly significant in 2025: revised guidance on the use of generative artificial intelligence by EUIs and new supervisory guidance on the role of DPOs.

In October 2025, we published revised supervisory guidance on the use of generative AI and the processing of personal data by EUIs. The revision reflects rapid technological developments and practical experience gained since the first guidance was issued. It provides clearer and more actionable direction to help EUIs design, deploy and use generative AI tools responsibly.

The revised guidance introduces a more precise definition of generative AI to ensure consistency of interpretation across EU administration. It also includes a new, action-oriented compliance checklist to support EUIs in assessing the lawfulness of their processing activities. In addition, the guidance clarifies roles and responsibilities, helping EUIs determine whether they act as controllers, joint controllers or processors in specific AI-related scenarios. Further sections provide detailed advice on lawful bases, purpose limitation and the handling of data subjects' rights in the context of generative AI systems.

In December 2025, we adopted new supervisory guidance on the role of DPOs in EUIs. This guidance builds on the principles set out in our 2018 position paper and on the experience gained since the entry into force of the Regulation (EU) 2018/1725, including insights from supervisory activities, surveys and workshops held within the EDPS-DPO network. Contributions from DPOs across EU administration played an important role in shaping the guidance.

The guidance provides clarification on several core aspects of the DPO function. It explains what is meant by direct reporting to the highest management level, addresses conflicts of interest in light of recent case law and practical use cases, and sets out how such conflicts can be prevented and managed. It also clarifies that, where relevant, the term of designation as DPO should be aligned with the duration of the underlying contract. Finally, it recalls the conditions that must be met for the dismissal of a DPO, reinforcing the importance of functional independence.

The guidance adopted in 2025 illustrates our commitment to providing EUIs with clear, practical and up-to-date supervisory tools. By addressing both emerging technologies and core governance roles, these guidelines support EUIs in strengthening accountability across the EU administration.

3.11. Supervisory cooperation with national DPAs, including within the EDPB

Supervisory cooperation with national DPAs is an essential element of effective and consistent enforcement of EU data protection law. In

2025, we cooperated with DPAs within and outside the EU/EEA, both in concrete cases and through structured cooperation frameworks, in particular within the EDPB. This cooperation supports a shared understanding of complex processing operations, facilitates consistent supervisory outcomes, and strengthens the protection of individuals' rights across the EU/EEA and beyond.

3.11.1. Cooperation in concrete cases

In 2025, cooperation with national DPAs focused on complex processing operations with cross-border relevance. We continued to exchange information with DPAs within and outside the EU/EEA on the use of cloud services by public bodies. In this context, we shared further information on our investigation and enforcement proceedings concerning the European Commission's use of Microsoft 365, supporting consistent supervisory approaches to similar cloud-based processing operations.

We also cooperated with two DPAs from EEA Member States following their requests for assistance. This cooperation concerned, first, the processing of personal data in tools provided by an EUI to other EUIs and to public bodies in EEA Member States, and second, the processing of personal data by an EUI in the performance of its tasks under EU law. Cooperation in both cases will continue in 2026, alongside further supervisory assessment of the processing operations concerned.

Where relevant, we also cooperated with national DPAs on concrete cases in the AFSJ, contributing our supervisory experience with EU-level systems and ensuring coherence between EU and national oversight.

3.11.2. Cooperation within the EDPB

Within the EU/EEA, we continued to contribute actively to the work of the EDPB. Drawing on our supervisory and enforcement experience, we provided input to support EDPB guidance, opinions and discussions on a range of topics, including anonymisation and pseudonymisation, data disclosures, safeguards for international transfers, controller–processor relationships and joint controllership.

By working together within the EDPB framework, DPAs and other competent authorities can address shared challenges more effectively and ensure consistent supervision of similar technologies and processing operations, particularly where these are carried out in the public interest.

3.11.3. Coordinated Enforcement Actions

In 2025, we continued to participate actively in enforcement actions under the EDPB's Coordinated Enforcement Framework (CEF). These actions aim to promote consistent enforcement of data protection rules across the EEA by focusing on selected topics of common relevance.

We participated in the 2024 CEF on the implementation of the right of access. As part of this action, we assessed how EUIs handle access requests through a survey and the analysis of complaint cases. The findings highlighted positive practices but also found recurring challenges: the generally low number of access requests received, decentralised handling of requests, difficulties in distinguishing access requests from other types of requests, challenges related to identity verification, and practical issues in balancing access rights with the rights and freedoms of others. These findings informed future supervisory priorities and were reflected in the EDPB report published in January 2025.

In 2025, we also took part in the fourth CEF, which focused on the right to erasure. Through a fact-finding exercise based on a survey, we examined how EUIs handle erasure requests, including the number of requests received and rejected and the procedures in place. The results showed that most EUIs receive a limited number of erasure requests, that many requests are rejected because the processing

is necessary for public interest tasks or legal obligations, and that while standard procedures are often in place, challenges remain in applying exceptions, handling combined access and erasure requests, and demonstrating accountability, in particular with regard to secure erasure techniques. These findings were shared with EUIs and their DPOs and will inform future supervisory and enforcement actions.

Finally, in October 2025, the EDPB selected transparency and information obligations as the topic for the 2026 CEF. We contributed to the preparatory work for this coordinated action and will continue participating in the planning discussions in 2026. A decision on our formal participation will be taken in the course of 2026, taking into account priorities and available resources.

Supervisory cooperation in 2025 demonstrates the added value of coordinated approaches to complex and cross-border data protection issues. By working closely with national DPAs and within the EDPB framework, we contribute to consistent enforcement, shared learning and effective protection of individuals' rights across the EU/EEA and within the EU administration.

3.12. Awareness-raising sessions

Awareness-raising is a key complement to our supervisory and enforcement activities. Through training sessions, presentations and exchanges with stakeholders, we support EUIs in building practical knowledge of data protection requirements and in anticipating compliance challenges. These activities help translate supervisory findings and guidance into day-to-day practice within the EU administration.

In 2025, the S&E Unit organised 30 awareness-raising actions. These took various forms, including training sessions, presentations, study visits, lectures and meetings with stakeholders. The activities addressed both horizontal data protection principles and topical issues arising from our supervisory work.

A significant focus was placed on the use of artificial intelligence in data processing activities, reflecting growing interest and concern across the EU administration. Other sessions addressed data subjects' rights, including access and erasure, as well as practical implications of outsourcing and procurement arrangements. We also provided targeted briefings on the closure of our investigation into the European Commission's use of Microsoft 365, helping EUIs understand the supervisory findings and their relevance for similar processing operations.

In addition, several sessions were dedicated to explaining our supervisory role and powers, supporting EUIs and stakeholders in understanding how supervision, investigations and enforcement activities are carried out in practice.

By investing in awareness-raising activities, we contribute to a preventive and informed approach to data protection compliance. The sessions organised in 2025 supported EUIs in strengthening internal capacity, applying supervisory guidance more effectively, and fostering a culture of accountability and respect for individuals' rights across the EU administration.

In 2025, the supervision and enforcement activities of the EDPS combined targeted oversight, guidance, cooperation and awareness-raising to address both established and emerging data protection challenges. Through supervisory opinions, investigations, audits, complaints handling, litigation and close cooperation with national authorities, we strengthened accountability and legal certainty across the EU administration. These actions not only resolved individual cases but also contributed to structural improvements in how personal data is processed. Building on this experience, the EDPS will continue to promote a consistent, effective and rights-respecting application of EU data protection rules in the years ahead.

CHAPTER FOUR

POLICY AND LEGISLATIVE CONSULTATION

The EDPS acts as an advisor to the European Commission, as the institution with the right of legislative initiative, and the European Parliament and the Council of the European Union, as co-legislators, on all proposed legislation impacting individuals' rights to privacy and personal data. In doing so, it contributes to shaping a safer digital future for the EU and its citizens.

This part of the EDPS's mandate is carried out by the Policy and Legislative Consultation Unit (P&C Unit). As the data protection and digital landscape continues to evolve, the EDPS's advice is increasingly sought after.

In 2025, the P&C Unit responded to 145 legislative consultations, in the form of opinions, formal comments and informal comments.

Opinions are typically issued in response to requests by the European Commission, which is legally obliged to seek our guidance on their legislative proposals that have an impact on personal data. We can also issue own-initiative opinions as part of our role as advisor on all matters relating to the processing of personal data.

Our formal comments address the data protection implications of implementing and delegated acts and therefore are usually more targeted and technical.

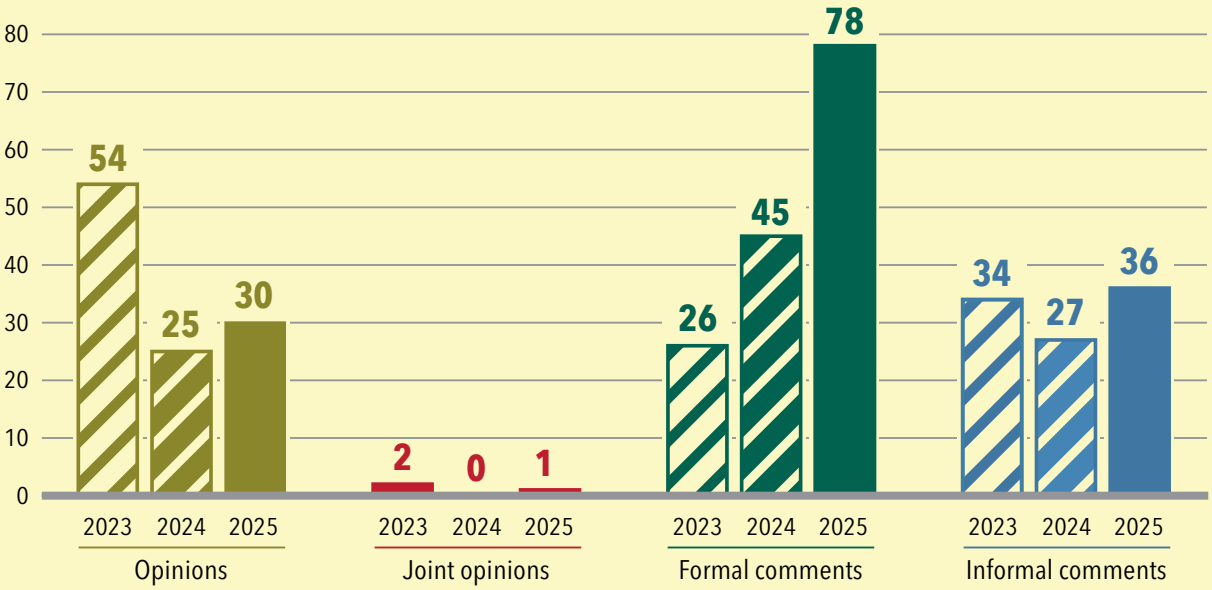
Informal comments are provided to the Commission before the adoption of a proposal that has an impact on data protection.

In 2025, we provided our advice across a range of topics, including Justice and Home Affairs (JHA), digital ID and credentials, targeted modifications of the General Data Protection Regulation (GDPR), and international agreements on tax compliance.

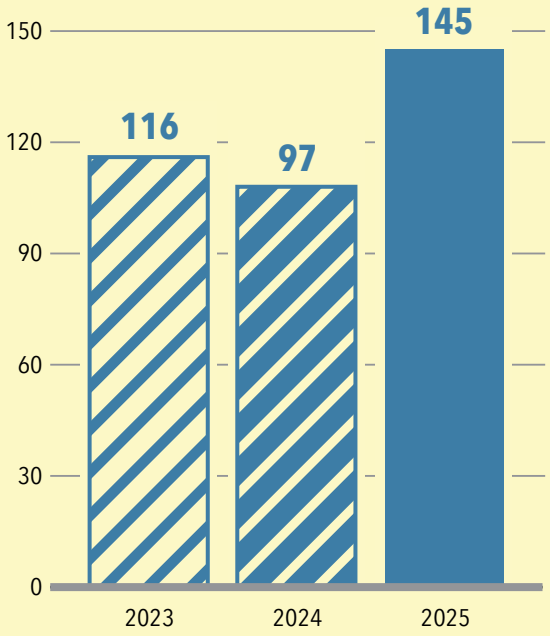
The number of requests for legislative consultation has remained very high in 2025. The statistics for 2025 also reflect the continuous

expectation of the European Commission's services to involve the EDPS by seeking our informal advice at the early stages of preparation of legislative or policy proposals.

Graph 5
Total replies to legislative consultation requests (2023-2025)



Graph 6
Categorised replies to legislative consultation requests (2023-2025)



4.1. Justice and Home Affairs

Justice and Home Affairs (JHA) is a specific policy area in which we routinely provide advice and recommendations. It covers matters such as combatting crime, judicial cooperation in criminal and civil matters, management of external borders, and asylum and migration. These tasks often involve the processing of individuals' personal data, including sensitive information, and so there is a need to ensure the protection of their fundamental rights and freedoms.

While this is our main goal, we approach each consultation with careful consideration of all issues at stake, in line with our core values of impartiality and pragmatism.

4.1.1. International law enforcement agreements

We provide advice in relation to multiple international agreements that envisage the transfers of personal data in the field of law enforcement. This is a sensitive area that presents specific risks for individuals and may lead to considerable negative impacts if their information is mishandled.

EU-USA opening negotiations on the exchange of information for security screenings and identity verifications

In September 2025, the EDPS issued Opinion 24/2025 on the negotiating mandate for a framework agreement between the European Union and the United States on the exchange of information for security screenings and identity verifications.

The aim of the recommendation adopted by the European Commission is to set out the legal structure and conditions for the sharing of such information between competent authorities of the EU Member States and the United States. On this basis, individual Member States would be empowered to sign bilateral agreements with the US Department of Homeland Security for the exchange of data from their national systems, called 'Enhanced Border Security Partnerships'. This information sharing has been made a pre-requisite to further participation in, and admission to, the US Visa Waiver Program.

The EDPS notes that the proposed framework agreement, once finalised, would establish an important precedent, as it would be the first EU agreement to entail the large-scale sharing of personal data, including biometric data (fingerprints), for the purpose of border and immigration control by a third country. Therefore, the EDPS stresses the need to ensure that the envisaged processing of personal data does not exceed the limits of what is strictly necessary and proportionate.

To this end, the EDPS makes a number of specific recommendations aimed at defining the personal and the material scope of the envisaged data sharing as narrowly as possible. Moreover, taking into account the specific prohibitions on certain data transfers laid down in EU law, any direct or indirect sharing and transfer of data from EU large-scale IT systems in the area of JHA – particularly those related to migration and asylum – must be strictly excluded.

The EDPS also makes important recommendations around accountability mechanisms, particularly the need for clear and specific justification of each query, the transparency of the envisaged processing, the corresponding information obligations of the competent US and EU authorities, and the availability of judicial redress in the United States regardless of citizenship.

EU signing of the United Nations Convention against Cybercrime

In September 2025, the EDPS issued Opinion 23/2025 on two proposals: one to authorise the signing, on behalf of the EU, of the United Nations Convention against Cybercrime, and the other to authorise the conclusion, on behalf of the EU, of the same convention.

The convention seeks to establish common rules at the global level to strengthen international cooperation in preventing and combatting cybercrime, as well as in the collection of electronic evidence for criminal investigations and proceedings.

The EDPS welcomes that, under the convention, states parties would not be obliged to transfer personal data if such transfers would breach their applicable data protection laws. In this regard, the EDPS underlined that EU Member States, when implementing and applying the convention, must carefully verify in each case whether the conditions set out in Chapter V of the Law Enforcement Directive are met before transferring personal data to a third country.

Furthermore, the competent authorities of Member States should ensure that transfers of personal data to third countries that are parties to the convention remain fully consistent with international human rights obligations and the fundamental rights of the individuals concerned. Where necessary, Member States should make use of the grounds available to refuse cooperation.

Finally, the EDPS recommended that the effects of the convention in practice should be carefully assessed and that data protection experts should be involved in its future reviews. Any possible future attempts to introduce offences incompatible with EU law or values should be firmly opposed.

Effective returns and re-admissions of third-country nationals illegally staying in the EU

In May 2025, the EDPS published an opinion on the proposal for a regulation establishing a common system for the return of third-country nationals staying illegally in the EU. The objective of the proposal is to provide Member States with simplified and common rules to enable the effective return and re-admission of third-country nationals illegally present in the EU.

In light of the impact of the proposal on concerned individuals' fundamental rights, including on their rights to privacy and to the protection of personal data, the EDPS considers that an in-depth fundamental rights impact assessment should be carried out to better identify and mitigate potential risks.

The EDPS also makes several specific recommendations, related to:

- the right to information given to individuals regarding the reasons for return decisions;
- the alignment of the proposal with the applicable EU legislation on data protection and other legal acts linked to the Pact on Migration and Asylum;
- safeguards in case of transfers to third countries of the personal data of concerned individuals.

The advice in the opinion is specific and clear. In particular, the EDPS recommends circumscribing the legal possibility to limit the disclosure of information about the factual reasons justifying a return decision. Such limitations should be applied only in exceptional cases, where it is strictly necessary, such as where disclosure would be contrary to the interest of State security. The EDPS also underlines the importance of ensuring that third-country nationals subject to a return procedure receive information about their rights as data subjects. In line with already adopted legal acts in the area of migration and asylum, the EDPS recommends introducing in the proposed regulation an explicit reference to the rights of individuals conferred by the applicable EU data protection law.

The EDPS also highlights the need for additional safeguards around transfers of personal data relating to the criminal convictions of third-country nationals. These transfers should be subject to a strict necessity test and must not lead to a death penalty, or any form of cruel and inhuman treatment. Furthermore, the EDPS recommends further specifying the conditions under which the personal data of children may be transferred to the third country of return, after a thorough assessment that the transfer is in the minor's best interest and will not endanger their well-being.

International agreements with third countries to fight crime with strong data protection safeguards

In 2025, the EDPS issued two opinions on agreements between the European Commission and two Latin American countries – Brazil (Opinion 2/2025) and Ecuador (Opinion 14/2025) – on data sharing to fight serious crime and terrorism. The agreements would facilitate the exchange of personal data between the EU Agency for Law Enforcement Cooperation (Europol) and the competent authorities of these countries.

The EDPS opinions assessed the data protection safeguards in these international agreements and, if necessary, provided advice on further developing them, so that individuals' personal data is protected according to EU standards.

The EDPS noted with satisfaction that previous recommendations on the negotiating mandates have been taken into account during the negotiations and reflected in the final texts, particularly related to storage limitation, the processing of special categories of personal data, automated decision-making, and the providing of information to data subjects.

Against this background, the EDPS concluded that the agreements with Brazil and Ecuador provide for adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals. At the same time, the EDPS stressed that the actual transfer of personal data from Europol to these Latin American countries should be conditional on the existence of an independent data protection authority (DPA) capable of exercising effective oversight over law enforcement authorities.

EU agreements on transfer of passenger name record data

In 2025, the EDPS issued several opinions on international agreements between the EU and third countries concerning transfer of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

PNR data is information collected from passengers by air carriers' and held in their reservation and departure control systems for commercial purposes. While useful for combatting terrorism and serious crime, the transfer of PNR data to third countries and the subsequent processing by their law enforcement authorities constitutes interference with the fundamental rights to privacy and data protection. Therefore, it must be necessary, proportionate, and subject to strict limitations and effective safeguards.

The EDPS issued three opinions on EU agreements on the transfer of PNR data with three Schengen-associated countries: Norway (Opinion 16/2025), Iceland (Opinion 15/2025) and Switzerland (Opinion 30/2025). Due to their Schengen Association Agreement with the EU, these countries are bound by certain Union legal acts, including Directive (EU) 2016/680 (the Law Enforcement Directive), in a similar manner as EU Member States. Our assessment of the draft agreements concluded that they contain the necessary safeguards required in order for it to be compatible with the EU legal framework on data protection.

In addition, the EDPS issued Opinion 28/2025 on the negotiating mandate for a similar agreement between the EU and Republic of Korea on the transfer of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. In the Opinion, the EDPS made specific recommendations on the need to strengthen the legal provisions on the right to information, including the right to individual notification when PNR data is disclosed (provided it does not jeopardise ongoing investigations), and on the mechanisms for possible amendments of the future agreement.

4.1.2. Large-scale IT systems and interoperability

Over the years, the EU has created a number of large-scale IT systems (LSITs) to support law enforcement, border management, migration and asylum in the Union, namely: the Entry/Exit System (EES), the Visa Information System (VIS), the European Travel Information and Authorisation System (ETIAS), the European Asylum Dactyloscopy Database (Eurodac), the Schengen Information System (SIS), and the European Criminal Records Information System for third country nationals (ECRIS TCN). Many of these systems have been operational for years, while others are in various stages of development. All of these systems will ultimately be closely interlinked with a single framework for interoperability, which has prompted regular updates of the applicable rules.

The EDPS has been paying special attention to this area in view of the potential impact of the processing of personal data in the systems on a very large number of individuals.

Formal comments on implementing and delegated acts related to EU LSITs in the JHA and their interoperability framework

In 2025, the EDPS issued 12 formal comments on different European Commission implementing and delegated acts related to EU LSITs in the JHA Council and their interoperability framework. The advice of the EDPS concerned:

- the functioning of the multiple-identity detector (MID), which creates and stores links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for travellers and combatting identity fraud;
- the user profiles in the European search portal (ESP), which facilitates the access by Member State authorities and Union agencies to the EU information systems and to the International Criminal Police Organisation (Interpol) databases;
- cross-system statistics;
- various other legal and technical aspects.

In addition, the EDPS issued formal comments on a draft Practical Handbook, prepared by the European Commission, on the implementation and management of the interoperability components. The Handbook offers a set of technical and operational guidelines, recommendations and best practices to be used by Member States' competent authorities in their daily work. In its advice to the Commission, the EDPS stressed the need to ensure effective exercise of data subjects' rights and to provide adequate information to the persons concerned, including through dedicated information campaigns.

4.2. Digital regulation

Digital regulation is a core policy area for the EDPS, covering advice and recommendations on personal data processing within the digital economy, including public sector digital services (e-government). EDPS activities in this field focus in particular on the development and implementation of the EU Digital Rulebook, where data protection and fundamental rights considerations must be integrated by design, notably the Digital Markets Act, the Digital Services Act, the Data Act, the Data Governance Act and the Artificial Intelligence Act.

Beyond these flagship instruments, the EDPS provides guidance across a broad range of interconnected sectors, including finance, taxation, competition law, digital identity wallets, cybersecurity, ePrivacy, and electronic communications. This cross-sectoral approach reflects the increasing convergence between digital regulation, data governance and fundamental rights protection in the EU's digital policy framework.

4.2.1. Targeted modifications of the GDPR: simplification of record keeping obligations

Together with the European Data Protection Board (EDPB), the EDPS issued in July 2025 a joint opinion on the European Commission's proposal for a regulation amending the GDPR, among other regulations.

The Proposal aims to modify Article 30 (5) of the GDPR, providing a derogation to the obligation to keep a record of data processing operations to enterprises or organisations under 250 employees – i.e. small and medium-sized enterprises (SMEs). Under the Proposal, the derogation would apply to an enterprise or organisation employing fewer than 750 people – i.e. a small mid-cap company (SMC) – unless the processing operation carried out is likely to result in a high risk to individuals' rights and freedoms, within the meaning of Article 35 of the GDPR.

In addition, the Proposal introduces definitions for SMEs and SMCs in Article 4 of the GDPR, and extends the scope of Articles 40 (1) and 42 (1), which refer to codes of conduct and certification, to include SMCs. These tools are currently designed to help enterprises and organisations demonstrate compliance with the GDPR, focusing on the specific needs of SMEs.

Regarding the organisations subject to the derogation, considering that the Proposal impacts legislation in other policy areas, the EDPB and the EDPS expect further clarifications on why the new threshold of 750 employees would be more appropriate under the GDPR, rather than the 500-employee threshold initially considered. In addition, the new exemption in Article 30 (5) refers to 'enterprises employing fewer than 750 employees' without referring to the newly introduced definitions of SME and SMC, which also includes financial criteria.

In order to ensure that the exemption will benefit SMEs and SMCs, the EDPB and the EDPS's joint opinion recommends referring to the newly introduced definitions of SME and SMC.

The EDPB and EDPS also ask the co-legislators to clarify in the Proposal that the term 'organisation', falling within the scope of the proposed derogation under Article 30 (5) of the GDPR, does not include public authorities and bodies.

4.2.2. EDPS opinions on international agreements

EU agreements with third countries on the exchange of financial account information

The EDPS was consulted on the proposals for Council decisions to sign and conclude amending protocols to the agreements between the EU and third countries on the automatic exchange of financial account information.

The amending protocols aimed to improve international tax compliance with Switzerland, Liechtenstein, San Marino, Monaco and Andorra, while ensuring that information-sharing with these third countries is aligned with the updated Common Reporting Standard developed by the Organisation for Economic Co-operation and Development (OECD), and with the new data protection framework.

As a European Economic Area (EEA) and European Free Trade Association (EFTA) country, Liechtenstein is not considered as a third country within the meaning of Chapter V of the GDPR. In the same vein, the international transfer of personal data from Member States to Andorra and Switzerland and do not require specific authorisations nor safeguards under Chapter V of the GDPR, by virtue of

an adequacy decision adopted by the Commission. Monaco and San Marino do require adequate safeguards to be included within the agreement since they do not enter into one of these two categories.

Proposal to conclude the Digital Trade Agreement between the EU and South Korea

Negotiations with the Republic of Korea, concluded in principle in March 2025, led to two Commission proposals for Council decisions on signing and concluding a Digital Trade Agreement on behalf of the EU.

The EDPS issued Opinion 27/2025 reiterating that personal data protection is a fundamental EU right that cannot be negotiated in trade agreements, questioned the need for further negotiations on cross-border data flows given South Korea's EU adequacy decision, and stressed that data protection and trade must follow separate tracks.

The EDPS recommended that the agreement clearly maintain safeguards for personal data and privacy, avoid affecting existing data protection frameworks, and strengthen references to horizontal data protection provisions. Additionally, the EDPS recommended that the agreement explicitly include personal data protection as a legitimate public policy objective, thereby allowing regulatory authorities to require access to source code to protect individuals' data, and not only for the more limited reasons currently listed.

Proposal to establish the EU position on the WTO Agreement on Electronic Commerce

In July 2024, the World Trade Organisation (WTO) Joint Initiative on Electronic Commerce concluded a stabilised text of the Agreement on Electronic Commerce (AEC). This amounted to what would be the first prospective global ruleset for digital trade once integrated into the WTO framework.

In February 2025, the European Commission proposed a Council decision to define the EU position on this topic, potentially enabling the EU to join a consensus in the WTO General Council on adopting the agreement.

The EDPS welcomed the inclusion of explicit personal data protection provisions (notably Articles 16 and 25) and recommended clarifying that the agreement cannot affect EU data protection and privacy safeguards, including EU/EEA data localisation requirements, where justified by fundamental rights.

Proposal for an agreement between the EU and the United Kingdom regarding the application of competition law

The EDPS issued Opinion 13/2025 on the European Commission's proposal for Council decisions authorising an agreement between the EU and the United Kingdom on cooperation in the application of their respective competition laws.

The EDPS highlighted that cooperation on competition enforcement involves exchanges of information that may include personal data, requiring full compliance with EU data protection and privacy standards.

The EDPS also stressed the need for clear safeguards, legal certainty, and robust guarantees in the agreement to ensure that any personal data processing and transfers between the EU and the United Kingdom fully respect fundamental rights to data protection and privacy.

4.2.3. European Digital Identity Wallet ecosystem

Formal comments on implementing acts to operationalise the European Digital Identity Wallet

In 2025, the European Commission consulted the EDPS on around seventeen draft implementing regulations and decisions under the eIDAS framework, which facilitates cross-border digital identity and authentication. The large majority of these were dedicated to operationalising the European Digital Identity Wallet (EUDIW) ecosystem.

These consultations covered the core building blocks required to make the wallet framework functional and interoperable across the Union. These included the registration and supervision of wallet-relying parties, the governance of attribute attestations and authentic sources, technical and organisational requirements for wallet services, and the interaction of these elements with EU-wide registries, catalogues and accreditation schemes. A smaller number of drafts addressed procedural or technical rules with more limited relevance to the wallet ecosystem.

Across these consultations, the EDPS's main findings were largely horizontal rather than specific to any particular draft. While acknowledging that most acts pursued legitimate interoperability and security objectives, the EDPS consistently emphasised the need to ensure that the implementing measures give concrete effect to data-protection-by-design principles embedded in the revised eIDAS framework.

In particular, the EDPS focused on clarifying roles and responsibilities within complex governance structures, preventing excessive or unjustified access to personal data by wallet-relying parties, and ensuring that registries, catalogues and supervisory mechanisms do not enable unnecessary data accumulation or indirect user tracking.

Where drafts were predominantly technical or procedural, the EDPS often concluded that no additional data-protection concerns arose. Where drafts structured core elements of the EUDIW ecosystem, the EDPS repeatedly emphasised safeguards to prevent excessive data access and accumulation, and to ensure that data minimisation, purpose limitation and user control are effectively enforced at ecosystem level.

4.3. Co-operation with the EDPB

As part of our responsibilities, the EDPS is both a member and provider of the Secretariat of the European Data Protection Board, the independent body in charge of ensuring consistent application of the GDPR and the Law Enforcement Directive across EU/EEA countries. To ensure consistent and impactful involvement of the EDPS as a member of the EDPB, we have set up an internal taskforce to coordinate our involvement and work on EDPB files.

As member of the EDPB, the EDPS is participating in monthly plenary sessions to develop guidance and make joint decisions with the other DPAs of the EU/EEA. EDPS representatives are also actively participating in the various EDPB expert subgroups and taskforces such as the Key Provisions Expert Subgroup, for which the EDPS is co-coordinator, as well as the subgroups in charge of international transfers, technology, financial matters, and law enforcement matters, amongst many others.

In this context, we regularly played an influential role within the EDPB as a lead rapporteur, co-rapporteur, or a member of the drafting team.

In recognition of the importance of the work carried out by the taskforce on the interplay between competition, consumer protection and data protection in 2023 and 2024, the EDPB decided to transform this taskforce into a new expert subgroup on cross-regulatory interplay and cooperation. The EDPS continued to co-coordinate this new expert subgroup in 2025, contributing decisively to the endorsement of the Joint Commission-EDPB

Guidelines on the interplay between the Digital Markets Act (DMA) and the GDPR by the EDPB Plenary in October 2025. The final version after public consultation will be published in 2026.

Through targeted and strategic involvement on certain key EDPB initiatives, we strive to represent the EU perspective, using our expertise as supervisor of EUIs, to ensure that EDPB's work is anchored in EU law, including in the case law of the Court of Justice of the European Union, and that EDPB applies the general principles of EU law.

We provided significant contributions to key EDPB documents adopted in 2025, including:

- Helsinki Statement on enhanced clarity, support and engagement;
- 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 Article 30(5) of the GDPR;
- Guidelines 3/2025 on the interplay between the Digital Services Act and the GDPR;
- Joint guidelines with the European Commission on the interplay between the Digital Markets Act and the GDPR;
- Position paper on the interplay between data protection and competition law;
- 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;
- Opinions 26/2025 and 27/2025 regarding the European Commission draft implementing decisions pursuant to Regulation (EU) 2016/679 and Directive (EU) 2016/680 on the adequate protection of personal data by the United Kingdom;
- Opinion 28/2025 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data by Brazil;
- Statement 4/2025 on the European Commission's recommendation on draft non-binding model contractual terms on data sharing under the Data Act;
- Guidelines 02/2024 on Article 48 of the GDPR;
- Statement 2/2025 on the implementation of the PNR Directive in light of CJEU Judgment C-817/19;
- Guidelines 01/2025 on pseudonymisation;
- Guidelines 02/2025 on processing of personal data through blockchain technologies;
- The EDPB comments on European Commission's Guidelines on Article 28 pf the Digital Services Act;
- Statement 1/2025 on age assurance;
- Best practices for requests for Article 64(2) opinions regarding matters of general application or producing effects in more than one Member State.

4.4. International cooperation

The EDPS actively fosters international cooperation to elevate data protection standards worldwide. We work closely with international organisations and fora to shape global privacy standards and tackle cross-border challenges. Our collaboration extends beyond the EU, engaging with organisations like the Global Privacy Assembly, the Council of Europe, OECD, and G7 DPAs (in the context of the Data Protection Authorities Roundtable). Through sharing expertise, we help promote a coherent regulatory approach that respects individuals' rights globally. This international engagement aims at promoting fair digital markets built on emerging technologies that are developed and deployed with strong safeguards. Such

efforts are crucial for addressing issues like AI and ethics, Data Free Flow with Trust (DFFT), and the harmonisation of regulatory practices across borders.

4.4.1. Global Privacy Assembly

In 2025 we contributed actively to the activities of the Global Privacy Assembly (GPA), an annual international forum that brings together more than 130 data protection and privacy authorities from across the globe.

The EDPS, jointly with the authorities from France, Hong Kong and South Korea, co-chairs the GPA working group on Ethics and Data Protection in AI (AIWG).

The EDPS also takes part in other GPA working groups, including the working groups on:

- global frameworks and standards;
- digital economy and society;
- data protection and other rights and freedoms;
- international enforcement cooperation;
- digital citizens and consumers;
- the role of personal data in international development aid, international humanitarian aid and crisis management;
- data sharing.

The 2025 edition was hosted by the Personal Information Protection Commission (PIPC) of South Korea from 15–19 September 2025 around the overall theme of 'AI in our daily lives: data and privacy issues'. The EDPS intervened in a panel on data protection in humanitarian action to discuss the challenges in the age of AI. The EDPS also shared some experiences from our cooperation with international organisations in a panel on developing mechanisms for cooperation and collaboration among DPAs and stakeholders.

On the occasion of this event, the GPA adopted three resolutions on:

- Digital Education, Privacy and Personal Data Protection for Responsible Inclusive Digital Citizenship;
- Collection, Use and Disclosure of Personal Data to Pre-train, Train, and Fine-tune AI Models, with the EDPS as co-sponsor;
- Meaningful Human Oversight of Decisions Involving AI Systems, with the EDPS as co-sponsor.

The EDPS also received the GPA Award in the Accountability category for two initiatives centred on preventing and managing data breaches: the Data Breach Awareness Campaign and the PATRICIA (Personal dATa bReach awareness In Cybersecurity Incident handling) tabletop exercise, both of which aimed at increasing awareness and response capacity to data breaches within EUIs.

Beatriz de Anchorena, Director of the Argentinian DPA and first non-European Chair of the Consultative Committee of the Convention 108 of the Council of Europe, received the Giovanni Buttarelli Award which was established to pay tribute to the memory of the late former EDPS.

4.4.2. EDPS Annual Workshop with International Organisations

Twenty years ago, the EDPS held its first International Organisations Workshop (IOW) – an informal but powerful forum where international organisations meet and share best practices, concerns and updates relating to the unique legal framework and specific data protection risks and challenges experienced by international organisations.

In 2025, the workshop was more relevant than ever, with personal data flowing faster and farther across borders than ever before, whether handled by humanitarian organisations, global health agencies or digital platforms. Held on 25-26 September 2025, the 20th anniversary

edition of the workshop, co-organised by the EDPS and the United Nations Educational, Scientific and Cultural Organization (UNESCO) in their premises in Paris, was attended by 180 representatives from 86 organisations.

Discussions focused on the most urgent privacy challenges faced by international organisations today. The agenda was designed to foster high-level exchanges on safeguarding personal data in a rapidly evolving geopolitical context, anonymisation of personal data, data transfers to and between international organisations and compliance of IT tools. Two breakout sessions on data protection risk assessments and data subject access requests were organised to enable participants to share best practices to embed awareness and accountability across international organisations.

In times of profound technological and societal evolutions linked to AI, participants also discussed the impact of the development and use of AI systems in international organisations, their expected benefits, and best practices developed to mitigate the risks posed by such systems.

Beyond technical matters, discussions also addressed values – how to combine efficiency with ethics, independence with interoperability, and security with fundamental rights. In our interconnected world, protecting privacy is essential for legitimacy and trust in public institutions.

4.4.3. G7 Data Protection Authorities' Roundtable

The G7 Data Protection and Privacy Authorities Roundtable convened on 18–19 June 2025, for a meeting hosted by the Office of the Privacy Commissioner of Canada (OPC), in Ottawa. The EDPS participated together with representatives from Canada, France, Germany, Japan, the United Kingdom and the United States. The EDPB and the EDPS represent the EU at such G7 DPA Roundtable meetings.

This annual event focused on the evolving data protection and privacy landscape, the implications of emerging technologies and the importance of cooperation among DPAs of like-minded countries to safeguard the data protection and privacy rights of individuals across jurisdictions.

Additionally, the G7 DPAs adopted a Communiqué and issued a Statement on promoting responsible innovation and protecting children by prioritising privacy. G7 DPAs emphasised that responsible innovation, where privacy considerations are built in at the start, can support confidence and trust in the digital world and be a driver of economic success and societal growth. The protection of children's best interests is particularly important with respect to the protection of children online.

The G7 DPAs also met virtually on 9–10 December 2025 to discuss the progress made throughout the year under the theme 'Championing privacy in a digital age: Collective action today for a trusted tomorrow'. The participating DPAs adopted a position paper on Data Free Flows with Trust (DFFT) which underlines that deepening practical discussions between regulators and collaboration between global stakeholders are essential to support innovation and growth while preserving privacy and data protection. The G7 DPAs also adopted the Action Plan for 2026 that commits to continuing to foster trust and support innovation that protects privacy, especially for children.

4.4.4. Council of Europe

The EDPS participates as an observer in the Consultative Committee of the Convention 108 (T-PD), the steering committee of Convention 108 in the field of data protection. In this capacity, we actively contribute to discussions and provide comments on the documents prepared by the T-PD.

The activities of the T-PD are diverse and concern topics of strategic importance for the EDPS, such as:

- artificial intelligence;
- oversight of intelligence services;
- contractual clauses in the context of trans-border data flows;
- privacy and data protection implication of the use of neurotechnology and neural data;
- the use of privacy enhancing technologies (PET) with regard to the processing of synthetic data and large language models.

Convention 108 has been modernised to address challenges resulting from the use of new information and communication technologies and to strengthen the Convention's effective implementation. Once it has obtained 38 ratifications, the Protocol modernising the Convention will enter into force as Convention 108+. The EDPS continues to support the efforts of the Council of Europe to promote the ratification of the Protocol. At the end of 2025, five ratifications were still missing for its entry into force.

The EDPS also represents the Global Privacy Assembly before the T-PD. Our role, in this respect, involves raising awareness of the relevant GPA actions among the T-PD members on the one hand, and advocating for their compatibility with EU data protection standards on the other hand.

Additionally, as part of the EU delegation, the EDPS participates in meetings of the Committee on Artificial Intelligence (CAI).

This committee developed the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, which is the first-ever international legally binding treaty in this field. The objective is to ensure that activities within the lifecycle of AI systems are fully consistent with human rights, democracy and the rule of law, while being conducive to technological progress and innovation.

In 2024, the CAI adopted the HUDERIA (human rights, democracy and the rule of law) methodology, a pioneering tool for conducting risk and impact assessments of AI systems. HUDERIA is a methodology to assist in identifying contexts and applications where AI systems could pose risks to human rights, the functioning of democracy and the rule of law, and to assess and mitigate those risks. In 2025, the CAI organised the HUDERIA Academy, a hands-on capacity building workshop, and established the HUDERIA Platform that brings together technical experts in the field.

4.4.5. Organisation for Economic Co-operation and Development

The EDPS participates as an observer and as part of the EU delegation to different working groups of the OECD, in particular the Working Party on Data Governance and Privacy (DGP), which is attached to the Committee on Digital Economy Policy, and the Working Party on Artificial Intelligence Governance (AIGO).

The OECD and the EU share common values regarding the need for the digital transformation to be human-centric and fundamental rights-oriented.

We provide, where necessary, comments to the working party on recommendations relating to the protection of privacy and data protection.

More specifically, the EDPS participates in the OECD expert community on Data Free Flows with Trust (DFFT) to support this initiative in the process of building trust surrounding data and its use across borders. This community gathers experts from governments, academia, civil society, business, and international organisations to provide project-based technical perspectives and evidence to the policy-oriented work of the OECD. The group focuses in particular on cross-border payments, enhancing legal transparency around data rules, and PETs.

4.4.6. European Conference of Data Protection Authorities

With the other DPAs of EU Member States and the Council of Europe, we met for the 33rd edition of the European Conference of Data Protection Authorities on 6–9 May in Batumi, Georgia. The 'Spring Conference' addressed data protection issues, emerging trends, and new developments relating to the rights to privacy and data protection.

The Spring Conference also serves as a way to promote cooperation between different European countries and exchange best practices. The Conference also adopted a Resolution on the Action Plan for Further Collaboration Activities.

4.4.7. EDPS-Western Balkans and Eastern Partnership Region: working together for data protection

Building on the first two fruitful meetings between the EDPS and the Western Balkans and Eastern Partnership in 2023 and 2024, we had the pleasure to welcome DPAs from the region to the third high-level event in 2025.

Representatives from DPAs and public institutions from Albania, Armenia, Bosnia and Herzegovina, Kosovo, Moldova, Montenegro, North Macedonia, Serbia and Ukraine were able to meet, share with and learn from each other on EDPS's premises in Brussels, Belgium for a 'Day at the EDPS'. The meetings fostered hands-on discussions on the details of the operational work of our institutions and interactive exchanges on our experiences, challenges and needs.

A wide range of topics of common interest were discussed, such as on best practices for advising the legislator – where the EDPS had the opportunity to present our Guidance for co-legislators on key elements to consider when drafting legislative proposals – as well as on the best practices and challenges in relation to technology monitoring.

There was a deep dive session on best practices and sharing of experiences on investigations, alongside some takeaways from our supervisory activities in the field of law enforcement and border management.

We also touched upon the central question of protecting personal data in the era of AI and presented the EDPS's new role and functions as supervisor of AI systems in EUIs under the AI Act.

These meetings highlighted the importance of collaborative learning. We gained insights into the compliance challenges faced by DPAs in these regions while sharing our own expertise. Strengthening these partnerships is essential, particularly as AI regulation and digital transformation accelerate. We remain committed to fostering cooperation, reinforcing privacy protections and shaping global standards for data protection.

4.4.8. Strasbourg EDPS Antenna

The EDPS decided to establish an EDPS antenna in Strasbourg in July 2022 to reinforce the EDPS's inter-institutional and international dimension. The Strasbourg office helps the EDPS to pursue three major objectives:

- establishing a closer and more stable link with the Council of Europe as a key stakeholder on the European and global stage;
- following more effectively the work of the European Parliament, in particular the plenary sessions, in which legislation that might have a major impact in terms of data protection is being discussed;
- facilitating cooperation with European agencies which have a presence in Strasbourg, such as eu-LISA.

The antenna office, initially operated as a pilot project for a duration of two years, is now established on a permanent basis. The presence of the EDPS in Strasbourg facilitates participation to various events and meetings organised at the European Parliament and at the Council of Europe in Strasbourg, as well as regular informal exchanges with various representatives of the Council of Europe, MEP assistants, the EU delegation before the Council of Europe, and other relevant stakeholders. Strengthening these links should remain at the core of the activities of the antenna in Strasbourg.

4.5. Other activities

4.5.1. High-Level Group for the Digital Markets Act

The EDPS is a member of the High-Level Group for the Digital Markets Act, alongside representatives of the EDPB. The group's role is to provide advice and expertise to the European Commission to ensure that the DMA and other sectoral regulations applicable to gatekeepers are implemented in a coherent and complementary manner. It may also provide expertise in market investigations into emerging services and practices.

In 2025, the HLG endorsed a joint paper on AI mapping out the regulatory interplay related to AI issues. The paper also proposed to explore closer cross-regulatory cooperation among competent authorities regarding the development and deployment of AI systems by gatekeepers.

Together with the EDPB, the EDPS priority in the high-level group is to ensure that personal data continues to be effectively protected in the constantly evolving digital landscape, advocating for clear guidelines to prevent misuse of data and to ensure that access to data is done under strict, proportionate and transparent conditions. The group's work helps maintain competitive digital markets while safeguarding individual privacy.

4.5.2. European Data Innovation Board

Alongside the EDPB, the EDPS is also a member of the European Data Innovation Board (EDIB). The EDIB is an expert group, chaired by the European Commission, established under the Data Governance Act (DGA), a regulation which aims to provide a framework for trustworthy voluntary data sharing across different fields.

The EDIB is set up to support a consistent approach to data governance across the EU by bringing together regulators and experts to provide guidance on data exchange, standardisation of some of the DGA's rules, and collaboration between its different actors.

The EDPS attended 3 meetings of the EDIB and contributed to discussions on the DGA from a data protection perspective.

4.5.3. EDPS guidance for co-legislators

In May 2025, the EDPS published its guidance for co-legislators, on key elements to consider when drafting legislative proposals and other acts that imply the processing of individuals' personal data.

With the guidance, the EDPS provides practical advice so that EU co-legislators can uphold the highest standard of the fundamental rights to privacy and data protection. The EDPS will continue to provide its recommendations to EU co-legislators where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.

In its guidance, the EDPS concentrates its advice to ensure that measures taken by the EU co-legislators are clear, precise and foreseeable, for the effective protection of individuals' personal data against the risk of misuse.

As such, the EDPS stresses the importance of carefully considering the following elements when drafting legislative and other acts entailing the processing of personal data:

- a clear specification of the objectives and purposes for which personal data is processed;
- clarity regarding the roles and responsibilities of those processing individuals' personal data;
- a demonstration of the necessity and proportionality of the envisaged processing of personal data in light of the objectives of a draft legislative proposal;
- delineation of the categories of personal data that are to be processed and the individuals concerned;
- a clear indication of the length for which personal data may be processed;
- appropriate safeguards in cases where personal data is to be disclosed to public authorities or other third parties;
- whether any envisaged restrictions on individuals' rights are legitimate and limited to what is strictly necessary in light of the objectives pursued.

4.5.4. High-Level Debate on Competition, Innovation and Data Protection

On 3 June 2025, the EDPS, the German Federal Commissioner for Data Protection and Freedom of Information and the Bavarian Data Protection Commissioner co-organised a high-level debate to reflect on recent developments relating to the EU's Digital Rulebook.

The event, kindly hosted by the Representation of the Free State of Bavaria to the EU, focused on the need for consistent and coherent implementation of the GDPR and the EU's Digital Rulebook. Participants discussed cooperation between digital regulators on the effective protection of citizens, fostering innovation, and supporting the Union's competitiveness.

CHAPTER FIVE

TECHNOLOGY AND PRIVACY

Through its Technology and Privacy Unit (T&P Unit), the EDPS monitors the evolution of technologies, and the digital landscape as a whole, to identify potential opportunities and risks for data protection.

The Unit's work is organized into three sectors:

- Technology Monitoring and Foresight tracks technological developments using a foresight-based methodology;
- The Digital Transformation Sector manages the institution's digital tools by integrating IT infrastructure from various EU institutions, bodies, offices and agencies (EUIs). It also procures open-source software to support specific EDPS tasks;
- The Systems Oversight and Technology Audits Sector conducts investigations and audits regarding the use of technology by EUIs when processing personal data. This work focuses primarily on large-scale IT systems (LSITs) within the Area of Freedom, Security, and Justice. This sector is also responsible for handling personal data breach notifications submitted by EUIs.

5.1. Technology monitoring and foresight

5.1.1. TechSonar report 2025-2026

With its yearly TechSonar publication, the EDPS aims to anticipate the impacts to individuals that might result from new technology trends and to broaden public awareness of these impacts.

In our TechSonar 2025-2026 report, we continued to focus primarily on AI-related technologies, exploring six emerging trends.

- Agentic AI refers to artificial intelligence systems that can autonomously make decisions, take actions and achieve goals with limited human intervention.

- AI companions are digital entities designed to simulate human-like conversations and relationships through artificial intelligence.
- Automated proctoring is used for remote monitoring and supervision of individuals during exams.
- AI-driven personalised learning customises content and the learning experience to the student's needs, using techniques such as machine learning, natural language processing, knowledge representation and learning analytics.
- Coding assistants help developers write and debug code.
- Confidential computing entails protecting data in a secured and isolated environment while it is being used.

This TechSonar issue comes with a series of six podcasts, one per trend, recorded in 2025 for publication in January and February 2026.

5.1.2. TechDispatch

While TechSonar provides an initial overview on technology trends, the aim of the aim of the TechDispatch reports is to delve deeper into emerging technologies and explain their impact in more detail.

Each TechDispatch provides factual descriptions of a technology, assesses its possible impact on privacy and personal data protection, and provides links to further recommended reading. With these reports and the associated video podcasts (see next section), we aim to foster ongoing dialogue on technology developments and data protection challenges while promoting data protection by design and by default within innovation processes.

In 2025, the EDPS published three TechDispatches, on federated learning, human oversight of automated decision-making (ADM), and digital identity wallets (DIW).

Federated learning presents a promising approach to machine learning, allowing multiple sources of data (devices or entities) to collaboratively train a shared model while keeping data decentralised. This technique is already being used in contexts where ensuring privacy and data protection is vital, such as healthcare, data spaces and autonomous transport systems.

Human oversight of automated decision-making concerns systems that not only execute tasks, but also make decisions that can affect individuals' lives and rights. The objective of this TechDispatch is twofold. Firstly, it examines common assumptions about how humans interact with and monitor decision-making systems, highlighting the overly optimistic nature of many of these assumptions. Accepting these assumptions uncritically can lead to inadequate or flawed implementations, posing significant risks – including harm to individuals and potential violations of fundamental rights. Secondly, it explores practical measures that providers and deployers of ADM systems can take to ensure that human oversight supports democratic values and safeguards human rights.

Digital identity wallets aim to provide users with an easy way to store their identity data and credentials in a digital repository so that they can access services in both the physical and digital worlds. This TechDispatch introduces the concept of a DIW and its associated privacy risks, as well as discussing relevant data protection by design and by default requirements and their implementation, including relevant technologies. Ultimately, the report assesses how the European Digital Identity Wallet (EUDIW), mandated by the eIDAS 2 Regulation which facilitates cross-border digital transactions and electronic interactions, fits within the framework outlined, fits within the framework outlined.

5.1.3. TechDispatch Talks

One of our priorities this year was to bring the tech world and its relationship with privacy closer to the public by expanding our reach to a wider audience. To this end, the EDPS has recorded and published two TechDispatch Talks (video podcasts) in 2025. These talks accompany the TechDispatch reports on federated learning and human oversight of ADM. The talk corresponding to the TechDispatch on digital identity wallets will be published in 2026.

5.1.4. IPEN event on Secure Multi Party Computation

The EDPS founded the Internet Privacy Engineering Network (IPEN) initiative in 2014 to promote and advance the state-of-the-art of privacy engineering. IPEN events bring together developers and data protection experts with a technical background from different areas, in order to build bridges and promote wider understanding of the technologies enabling the protection of personal data. Since then, the EDPS has organised one or two IPEN events a year on topics such as digital identity, central bank digital currencies, explainable AI and synthetic data.

On 21 October 2025, the EDPS and the Goethe University Frankfurt hosted an IPEN event on the topic of secure multi-party computation (SPMC), which is emerging as a key privacy-enhancing technology. By enabling joint computation on private data without revealing it,

SMPC promises to transform data processing in sensitive domains like finance, healthcare, and national security. 175 participants attended either in person or online, and the topics touched upon included:

- the potential of SMPC to enable collaboration without sacrificing privacy;
- the reduction of systemic risk of cyber incidents;
- challenges related to performance and interoperability;
- legal and ethical concerns.

5.1.5. Cooperation with the EDPB in assessing the impact of technology

As a member of the European Data Protection Board (EDPB) and as a provider of its secretariat, the EDPS supports them in various tasks. The T&P Unit takes an active part in assessing technologies' impact on fundamental rights when personal data is processed.

In 2025, topics on which we cooperated with the EDPB ranged from the use of anonymisation and pseudonymisation in the processing of individuals' personal information, to the use of blockchain, the use of biometrics for physical access control, and the assessment of data protection risks deriving from the use of artificial intelligence.

5.1.6. International Working Group on Data Protection in Technology

The EDPS, represented by the T&P Unit, remains actively involved in the International Working Group on Data Protection in Technology (IWGDPT), also called the Berlin Group, which observes trends and developments in the technological sector. The working group is composed of representatives of data protection supervisory authorities from across the globe, as well as independent experts from various sectors, including public authorities, private organisations, academia and civil society. The IWGDPT provides practical advice on privacy-friendly and privacy-enhancing solutions with regard to emerging data-related technologies and services.

This year, the EDPS took part in two Berlin Group meetings, one held in Tbilisi, Georgia, and another in Montevideo, Uruguay. Among the working papers discussed were those on global opt-out preference signals and related technologies, extended reality, and confidential cloud computing, the latter for which the EDPS contributed as co-rapporteur.

5.2. Overseeing IT systems and auditing technology

5.2.1. EDPS AI risk management guidance

In 2025, the EDPS published new guidelines on AI systems, to provide insights and practical recommendations to help identify and mitigate common associated technical risks.

The development, procurement and deployment of AI systems involving the processing of personal data by EUIs raises significant risks to data subjects' fundamental rights and freedoms, including, but not limited to, privacy and data protection.

The data protection regulation for EUIs (Regulation (EU) 2018/1725) requires them to identify and mitigate these risks, and to demonstrate how they did so. These guidelines are intended to assist EUIs acting as controllers in this task. More specifically, they focus on the risk of non-compliance with certain data protection principles such as fairness, accuracy, data minimisation, security and data subjects' rights.

5.2.2. Website Compliance Awareness Campaign pilot

In 2018, the EDPS developed the Website Evidence Collector (WEC) tool for its remote website audits. The EDPS made this tool publicly available so EUIs' controllers and data

protection officers (DPOs) could identify potential issues and areas of improvement on their websites. However, despite the WEC's availability, the knowledge and use of the WEC by EUIs was very limited.

In 2024, the EDPS launched a pilot of the website compliance awareness campaign (WCAC). In this pilot, the EDPS has run the WEC twice a year on one selected website of each of the EUIs under its remit (which total around 70). The EDPS conducted the first wave of WEC runs in October 2024.

In 2025, the EDPS completed the second and third waves of the WCAC, finalising the pilot. After each wave, institutions received individual factual reports and a review workshop was organised. In 2026, the EDPS will assess the results of the pilot and decide on how to expand the scope of the campaign to cover more EUI websites. In addition, the EDPS organised two training sessions to provide the recipients with a better understanding of the factual data included in the WCAC reports.

This awareness-raising initiative around potential compliance issues was promoted by the EDPS to support controllers in fulfilling their accountability obligations under Regulation (EU) 2018/1725. The EDPS also participated in training sessions organised by other institutions with a similar goal.

5.2.3. WEC online deployment

Despite the WEC's availability as open-source software, its use by EUIs has been very limited. This seems to stem from the lack of a graphical user interface and the difficulties of installing on corporate devices software that has not been vetted by EUI's cyber security teams. The expense and length of the process was a major barrier to successfully vetting the niche WEC software.

To address these two issues, in July 2025, the EDPS began to offer the EDPS WEC tool as an online service (WEC Online). This service is accessible to staff working for EUIs from devices connected to their corporate network. WEC Online does not require software installation in users' devices, and it provides a user-friendly web interface that authenticates users through EU Login.

WEC Online enables automated collection of digital evidence from websites and the generation of summary reports containing information it collects:

- the use of encryption (HTTPS/SSL) when connecting to the website;
- the presence of web forms that submit non-encrypted data;
- links to common social media platforms;
- third-party requests made by the website;
- use of content security policies (CSP);
- cookies present on the website;
- potential web beacons on the website;
- HTML5 local storage usage.

WEC Online allows EUIs to run by themselves the same checks the EDPS can perform. This will enable EUIs to check the results of a website update or a planned improvement action.

The EDPS also publishes the WEC online source code, under EU Public License (EUPL).

5.2.4. Large-scale IT systems

Large-scale IT systems technology audits

The European Union has established a number of large-scale IT systems (LSITs) whose supervision is shared between the national data protection authorities (DPAs) and the EDPS. In this context, the T&P Unit regularly carries out audits of these systems, as provided for in the legal instruments establishing these systems, and in accordance with internationally recognised auditing standards.

In October 2025, the EDPS transmitted the final audit report on the Visa Information System (VIS) to eu-LISA (the European Union Agency for the Operational Management of Large-Scale IT Systems), the European Commission, the European Parliament, the Council of the European Union, and national DPAs. The audit fieldwork had been conducted in December 2024 and focused on selected aspects of IT security management, including vulnerability management, the handling of personal data breaches and security incidents, user account management, and logging and monitoring practices.

In December 2025, the EDPS conducted an audit of the Eurodac information system at the eu-LISA premises in Strasbourg. The EDPS is legally required to audit eu-LISA's management of Eurodac at least every three years. The corresponding audit report is expected to be finalised in 2026.

Since 2024, the EDPS has also been under a legal obligation to audit every five years the processing of personal data in the Customs Information System (CIS). The CIS is an LSIT that processes customs information for the purpose of preventing, investigating and prosecuting breaches of Union customs and agricultural legislation. The European Anti-Fraud Office (OLAF) is responsible for the development and operational management of CIS on behalf of the Member States.

In November 2025, the EDPS conducted an audit of CIS and the Files Identification Database (FIDE), both operated by OLAF. The audit focused on the use of CIS and FIDE in criminal investigations where OLAF acts as a processor, and covered security, confidentiality, logging, and data protection-related processes. The audit report is expected to be finalised in early 2026.

Notification of Security Incidents affecting Large-Scale IT Systems

Under the applicable legal framework, the authorities of EU Member States, Europol, Eurojust, and Frontex are required, in specific cases, to notify, without undue delay, the European Commission, eu-LISA, the competent national supervisory authority, and the EDPS of any security incident that has affected an LSIT under their responsibility. eu-LISA is also obliged to notify the European Commission and the EDPS of any security incident concerning the relevant central system.

In 2025, the EDPS established a new process for receiving the security incident notifications affecting LSITs, applicable to eu-LISA, Frontex, Europol, Eurojust, and Member State authorities. This process is supported by a dedicated reporting form designed to ensure that a minimum set of essential information is consistently provided to the EDPS. The EDPS cooperated closely with eu-LISA in the development of this form to ensure alignment with eu-LISA's existing security incident reporting mechanisms and to minimise the administrative burden on reporting entities.

To raise awareness of the applicable reporting requirements and procedures, the reporting form, together with guidance on how to notify a security incident to the EDPS, was published on the EDPS website. It was also presented to several stakeholders such as the Coordinated Supervisory Committee (CSC) of the EDPB ([9]) and eu-LISA's Security Officers Network (SON) ([10]).

5.3. Digital transformation

The EDPS continues its digital transformation, under the leadership of the T&P Unit. In 2025, we continued support for EU Send, a communication tool managed by the European Commission to facilitate the secure exchange of sensitive, non-classified data such as information on health, having expanded its use to new use cases.

We also streamlined the IT support by starting using the Service Now application used by ITEC (the European Parliament's IT support service). The EDPS now benefits from a single IT helpdesk portal regardless of whether the service is provided by the EP or the EDPS. Additionally, we collaborated with the European Commission and with the EP to expand the scope of the information shared via SECABC (a solution that enables encrypted email communication across all participating EUIs), to enhance interoperability with other EUIs.

5.3.1. Meeting of the Interinstitutional Committee for Digital Transformation

The Interinstitutional Committee for Digital Transformation (ICDT) is a collaborative body, currently chaired by the Court of Justice of the European Union (CJEU), established to coordinate and align digital transformation efforts across the European Institutions. Its main purpose is to foster interinstitutional cooperation in areas such as digital governance, artificial intelligence, data management, and cloud infrastructure, aiming to have all EU entities move consistently towards secure, interoperable, and more citizen-centred digital solutions.

By bringing together representatives from the European Commission, the European Parliament, the Council and other EUIs, the ICDT provides a forum where strategic discussion and decision-making can take place on digital initiatives that impact multiple institutions. The T&P Unit usually represents the EDPS in the ICDT.

On the 17 December 2025, with the operational coordination of the Digital Transformation sector, the EDPS hosted the ICDT plenary meeting. At the meeting, the Supervision and Enforcement Unit presented the closure the EDPS's investigation into the European Commission's use of Microsoft 365. The Artificial Intelligence (AI) Unit presented the preliminary results of the mapping of possible high-risk AI systems in EUIs, and a pilot AI sandbox project.

([9]) The CSC is a group of national supervisory authorities and the EDPS, and coordinates supervision of LSITs and EUIs, in accordance with Article 62 of Regulation (EU) 2018/1725 or with the EU legal act establishing the LSIT or EUI.

([10]) The SON is a working group of security specialists representing eu-LISA, the European Commission, other EU bodies and EU Member States. It provides support to the eu-LISA Management Board and Advisors Groups regarding security, safety and business continuity related matters.

5.3.2. EDPS Public-Key Infrastructure system

The EDPS relies on its own Public-Key Infrastructure (PKI) system to manage digital certificates for authenticating staff in the EDPS Case Management System (CMS).

The Digital Transformation sector identified the need to update and modernise this critical infrastructure in 2023 and started a project that involved researching and testing exporting and importing the data to a new version of the underlying software.

During 2024 and the first half of 2025, we tested several iterations and assessed several alternatives for the underlying software and for hosting it, concluding that the most adequate alternative is an updated version of the same software, hosted in the EP's infrastructure with additional security controls that raise its level of cybersecurity.

We concluded the installation, configuration and testing in August 2025, conducted a test pilot between September and November 2025, and initiated the migration in December 2025.

We expect to conclude this project in May 2026.

5.3.3. Updating tech support for the EPBS and EDPB videoconferencing rooms

In 2019/2020, the EDPS installed, with the support of an external contractor and some equipment provided by ITEC, two video conferencing rooms: the Giovanni Buttarelli room (ground floor) and the EDPB's room (first floor).

However, as the initial installation was not carried out by ITEC and due to the mixed configuration, ITEC was limited in its ability to provide support beyond basic network connectivity, and the EDPS/EDPB Secretariat faced challenges in procuring maintenance. Moreover, with some equipment reaching the end of its life, replacement and maintenance were necessary to permit reliable and secure meetings.

When this situation was identified, in late 2024, a joint effort between the Technology and Privacy, Information and Communication, and Human Resources, Budget and Administration Units, and the EDPB Secretariat, in close cooperation with ITEC, was set up to find a solution. It was decided that ITEC would replace the equipment that is not under its control and guarantee the regular business operation in case of problems.

During 2025, after a lengthy process, ITEC identified a solution involving DG LINC and DG INLO (the Directorates-General for Logistics and Interpretation for Conferences, and for Infrastructure and Logistics) that would allow them to provide full support and maintenance for both videoconferencing rooms, and to replace obsolete equipment, with the assistance of a budgetary contribution from the EDPS.

As of 2025, both rooms are fully supported by ITEC and the obsolete equipment on the ground floor room has been replaced. We expect to conclude this project by the 3rd quarter of 2026 with the replacement of the obsolete equipment in the EDPB's videoconferencing room.

5.3.4. Assessing and piloting AI tools at the EDPS

During 2025, the T&P Unit supported the Artificial Intelligence Unit's initiative to secure early access to the Directorates-General for Digital Services (DG DIGIT)'s 'GPT@EC' AI tool.

In close collaboration with the Artificial Intelligence Unit, the EDPS DPO and DG DIGIT, the EDPS signed an amendment to the service level agreement between the EDPS and DG DIGIT to afford early access to GPT@EC to 30 users from the EDPS.

The T&P Unit supported this initiative from the operational point of view and the Digital Transformation sector took responsibility for managing access to the 30 users.

In December 2025, DG DIGIT onboarded all staff of the EDPS and the EDPB Secretariat to GPT@EC, and we expect the EDPS to begin piloting this tool in 2026.

5.4. Verifying and supporting EUIs in the management of personal data breaches

5.4.1. Global Privacy Assembly award

In 2025, the EDPS received international recognition at the Global Privacy Assembly (GPA) Awards, where it was awarded in the Accountability category for two initiatives aimed at strengthening the prevention and management of personal data breaches within EUIs. The GPA brings together more than 130 DPAs worldwide and recognises outstanding achievements in professionalism, transparency and accountability.

The award acknowledged the Data Breach Awareness Campaign, which supports EU institutions in assessing and improving their data breach management procedures, and the PATRICIA exercise, a tabletop cybersecurity exercise conducted in cooperation with European Union Agency for Cybersecurity (ENISA), with the Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies (CERT-EU) participating as an observer. This exercise enabled participants to test responses to realistic personal data breach scenarios and to enhance coordination in cybersecurity incident handling.

This recognition highlights the EDPS's continued commitment to fostering a culture of accountability, promoting cooperation and capacity-building, and strengthening data protection practices across EUIs. The EDPS will continue to engage with European and international partners to ensure that data protection frameworks evolve in line with emerging risks and technological developments.

5.4.2. PATRICIA II

Following a successful pilot in 2024, the EDPS organised the second tabletop cyber exercise, at the European Parliament's Info Hub in Brussels. PATRICIA II – Personal dATa bReach awareness In Cybersecurity Incident hAndling – was designed to enhance awareness and coordination in managing personal data breaches resulting from cybersecurity incidents. IT professionals, security officers, and DPOs from across the EUIs participated in PATRICIA II to simulate and analyse their coordinated responses to a complex cyberattack scenario involving personal data breaches. This year's session involved eight EUIs, while CERT-EU participated as an observer and provided expert input during discussions relevant to their mandate.

The event was split into two sessions. The first part simulated real-world cybersecurity incidents, challenging teams to react using their internal processes, assess risks, and coordinate their response. The second session was a debriefing, where participants reflected on their decisions, examined the effectiveness of their responses, and identified areas for improvement.

After analysis of the responses and participants' feedback, EDPS recommended improving internal coordination and shared understanding of the interplay between different roles managing personal data breaches, harmonising internal processes relating to breach management and internal reporting tools, and promoting interdisciplinary training and awareness, to ensure common understanding of security and personal data breach concepts.

Overall, the exercise underlined the importance of a coordinated approach with clearly defined roles under all relevant legal frameworks, as well as the need for continuous training, improved information sharing, and learning from past incidents.

Looking forward, the EDPS plans to adapt the exercise for larger, multi-DG organisations such as the European Parliament, European Commission, and Council of the European Union, where data protection structures are more complex. EDPS aims to develop new scenarios for future editions, invite additional EUIs that have not yet taken part, and integrate participant feedback to ensure even more realistic and challenging exercises, including the involvement of joint controllers.

5.4.3. Legal obligations with personal data breaches

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to transmitted, stored or processed personal data of individuals. The impact of a personal data breach can be far-reaching, such as identity theft or damage of an individual's reputation.

Under Regulation (EU) 2018/1725 (the Data Protection Regulation for EUIs), all EUIs have a duty to notify personal data breaches to us, unless a risk to the affected individuals is unlikely. All EUIs must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to pose a high risk of adversely affecting individuals' rights and freedoms, the EUI must also inform the concerned individuals without undue delay.

These obligations apply also for breaches on 'operational personal data'. While Chapter 9 of Regulation (EU) 2018/1725 introduces data breach notification requirements for operational personal data, additional requirements may be introduced in regulations that apply specifically to certain EUIs, such as Europol, Eurojust or the European Public Prosecutor's Office (EPPO).

The 2025 administration of incoming personal data breach notifications has seen a slight decrease in number compared to the previous year alongside some interesting compliance challenges (e.g. interplay with AI). The notification handling process of all cases is sufficiently mature to enable the EDPS to successfully manage the review and closure of cases in a structured and efficient manner. Indeed, for 2023 and 2024, 99% of cases are now closed. Concerning the cases of 2025, more than 35% are closed and 45% are on track to be closed in the first quarter of 2026.

5.4.4. Emerging challenges in the personal data breach management domain

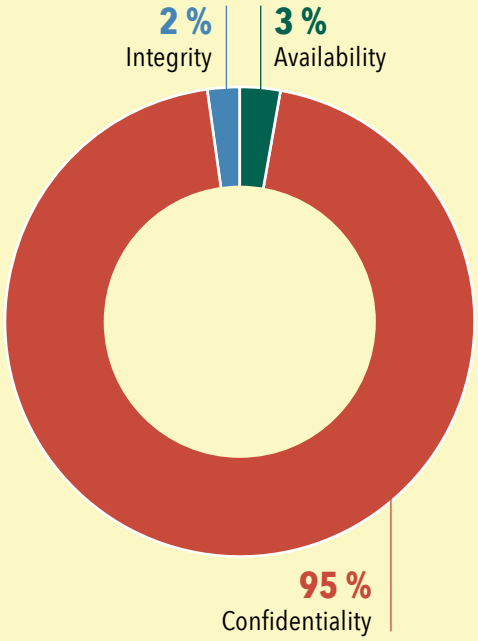
Following exchanges with EUI DPOs and in light of the evolving legal framework, the EDPS has identified a number of challenges in the area of personal data breach management.

The increasing use of artificial intelligence tools is relevant in this context. The widespread availability of tools such as ChatGPT or Gemini has led staff members in EUIs to use such tools both in their private capacity and in the course of their professional activities, in some cases without prior authorisation from the controller. This situation forms part of the so-called "shadow IT" phenomenon and should be duly reflected in organisations' risk assessments. Controllers should therefore reinforce their IT governance and oversight mechanisms and develop robust IT security and resilience strategies.

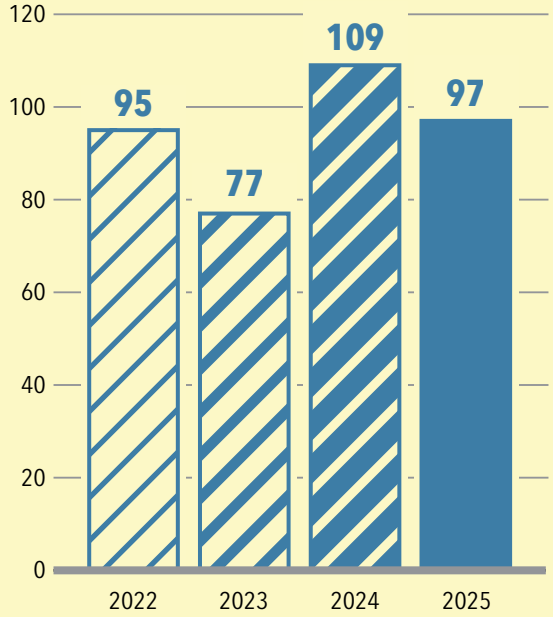
5.4.5. By the numbers: personal data breaches in 2025

In 2025, we received and assessed 99 data breach notifications submitted by EUIs under Article 34(1) of Regulation (EU) 2018/1725, among which two were deemed inadmissible. This amounted to an almost 11% drop compared to 2024. Out of the 97 admissible data breach notifications in 2025, 92 cases were primarily breaches of confidentiality, whereas three cases were breaches in the availability of data and the rest concerned an integrity issue.

Graph 7
Primary types of data breaches

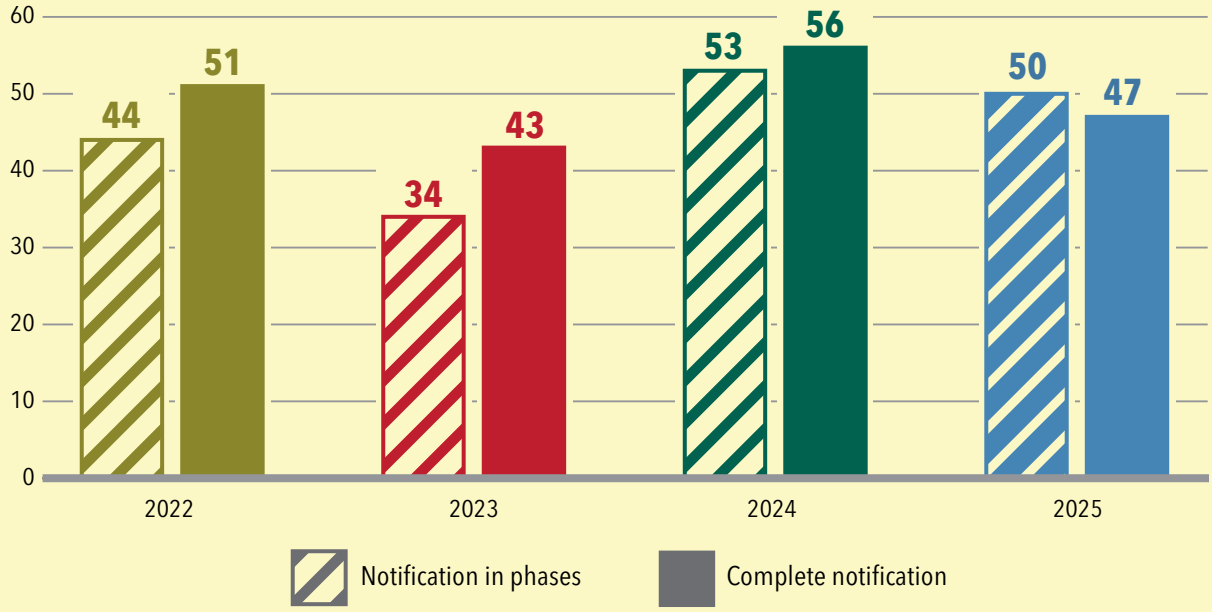


Graph 8
Total admissible data breach notifications (2022–2025)



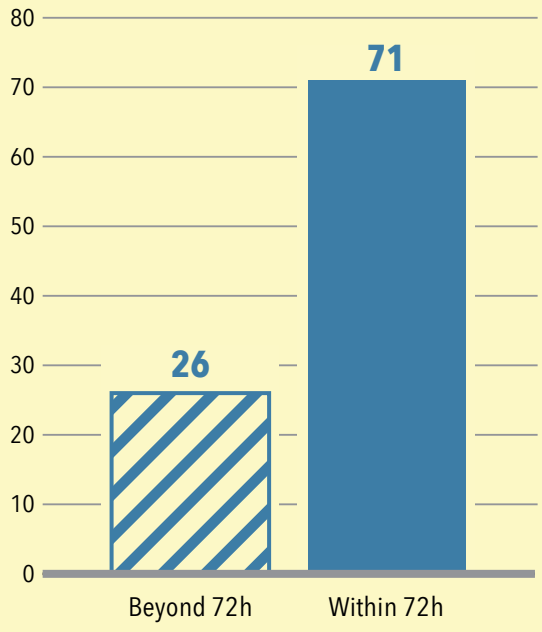
In 2025, of the 97 admissible personal data breach notifications from EUIs, we received 47 complete notifications and 50 in phases. By the end of 2025, not all notifications in phases had yet been finalised. As shown below, in 2025 comprehensive notifications were, for the first time, fewer in number than notifications in phases.

Graph 9
Type of data breach notification – complete v. in phases (2022-2025)



71 notifications were submitted within 72 hours, while 26 notifications were delayed by the controllers due to various reasons. In some cases, the delay was justified, as for example for cases with ongoing investigations trying to identify how individuals' personal data were affected. In some other cases, delays occurred due to the lengthy internal procedures of the controllers concerning the final approval of the notification. In the latter case, we advise the EUIs to review, simplify and document their internal processes to meet the legal deadline. In comparison to 2024, no changes are observed in terms of the proportional rate between the 72-hour thresholds ([11]). This observation supports the interpretation that controllers demonstrate continuous efforts to comply with the legally set deadline.

Graph 10
Notifications received within/beyond 72-hour threshold



([11]) The proportional rate of the total number of delayed notifications out of the total number of data breach notifications is 26% for both years 2024 and 2025.

In 2025, once again, human error remained the most common root cause behind personal data breaches with a 24% increase compared to the previous year. The most common errors are sending emails to unintended recipients, attaching files disclosing personal data, and placing incorrectly masked documents on public websites.

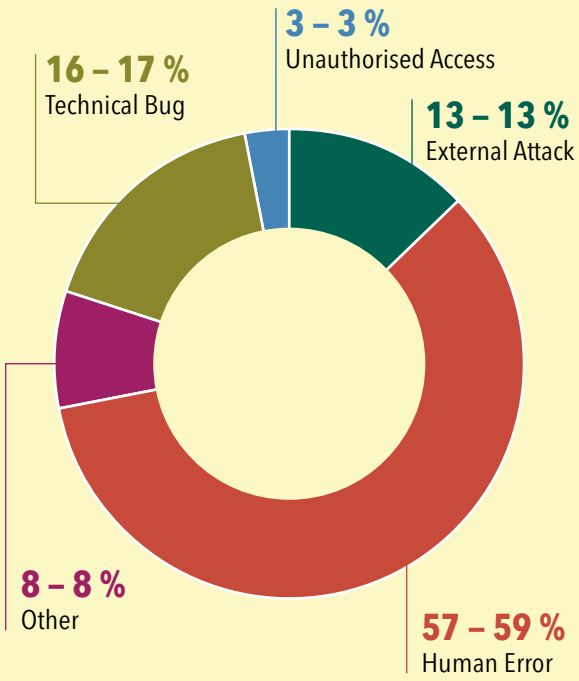
Personal data breaches originating from a technical bug were second most common, decreasing by 27% compared to 2024. These bugs arise from, for example, the misconfiguration of access rights or other incorrectly configured features, due to a lack of testing of the tool before deployment or a lack of regular review afterwards.

Contrary to common expectations around cyber-attacks against public institutions ([12]), 2025 saw a decrease of more than 50% in personal data breaches caused by external attacks against EUIs.

Alongside exploitable weaknesses such as poor security design or inadequate patching of internet-facing systems, external attackers targeted IT assets or platforms holding large amounts of data (e.g. mail servers). This could be interpreted as evidence of the value placed on bulk data, including personal data. Personal data has the potential to be monetised or reused in quasi-immediate secondary attacks.

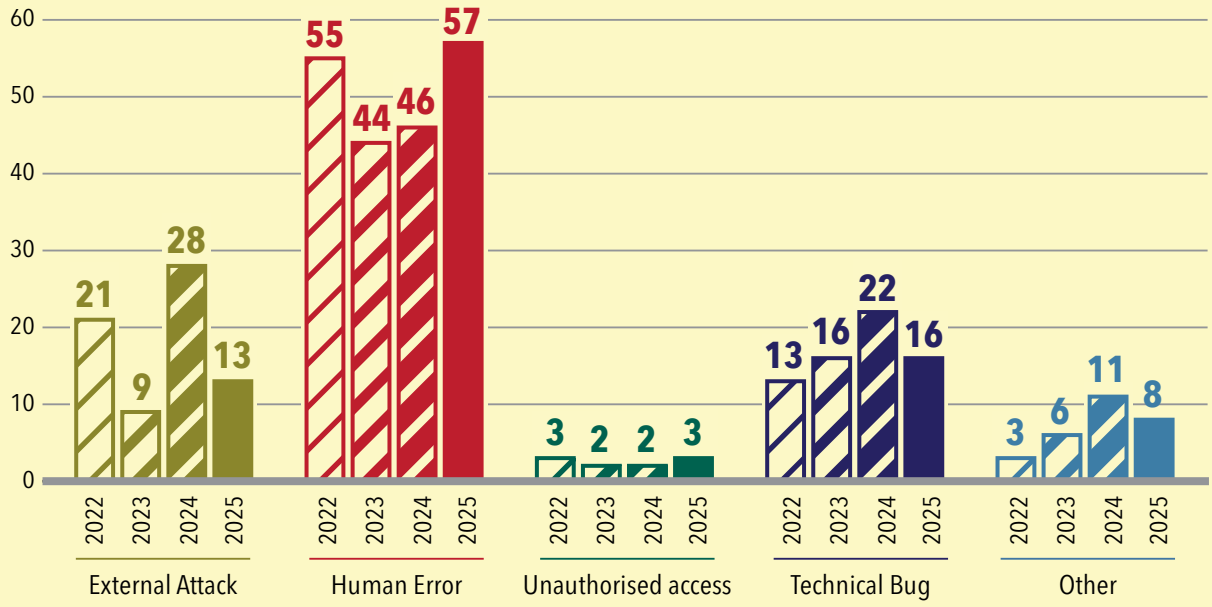
Under the "Other" category, the root cause mostly relates to the loss or theft of mobile devices.

Graph 11
Personal data breach root causes

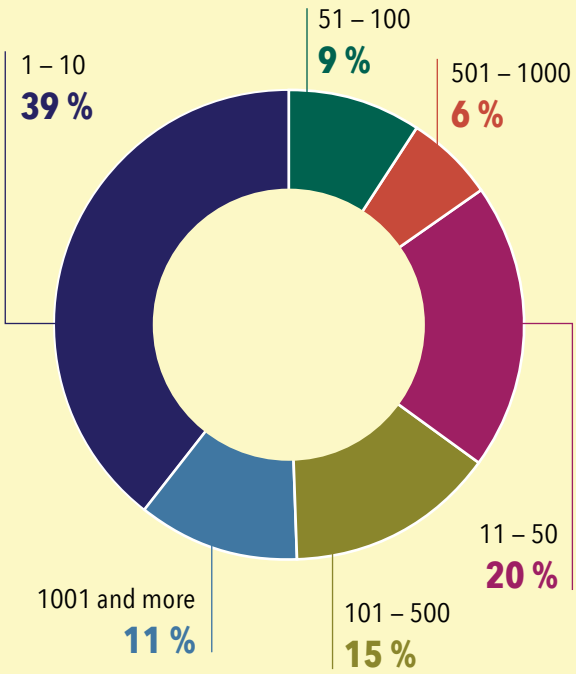


([12]) Public administration was identified as the most targeted sector in the EU (38.5%), dominated by low-impact DDoS, (94.8%), with ransomware particularly affecting municipalities. ENISA Threat Landscape Report (October 2025).

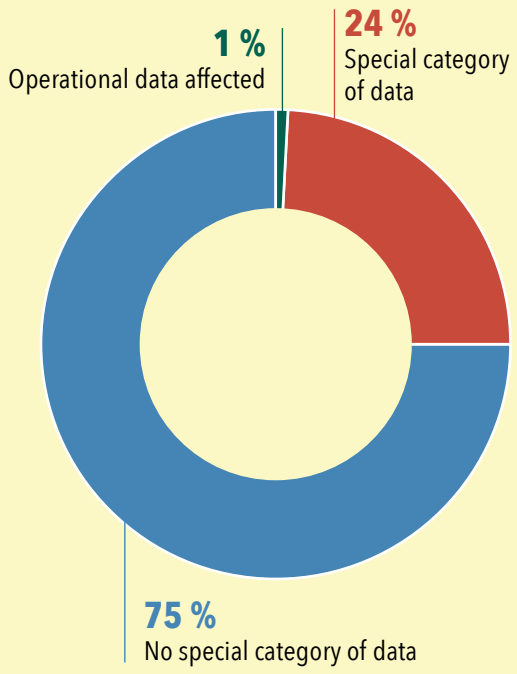
Graph 12
Personal data breach root causes (2022–2025)



Graph 13
Number of data subjects affected

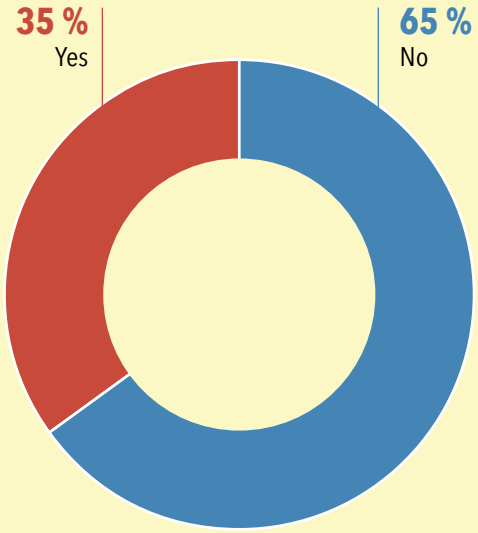


Graph 14
Data types affected



24% of admissible personal data breach notifications received in 2025 concerned special categories of data, especially health data, due to errors when communicating medical files via email or storing these files in the wrong subfolders of the document management tool. In these circumstances, we recommend that EUIs raise their staff and contractors' awareness on the matter and consider additional safeguards (e.g. regularly reviewing user access and permissions) to avoid human error and reduce data exposure. In 1% of personal data breach cases, operational personal data was impacted. Under 'operational data', the categories of persons affected includes suspects and individuals under investigation, as well as information related to officers being assigned specific tasks. Regarding the personal operational data breach notification received by the EDPS, no special categories of data were concerned.

Graph 15
Data subjects notified – yes v. no



5.4.6. Communication to individuals in 2025

In 63 cases, EUIs decided to communicate the personal data breach to the individuals concerned. While some controllers carried out this communication in response to the identification of high risks for the affected individuals, others chose to notify data subjects as a matter of transparency. In these latter cases, the EDPS observed that the communication process was often treated as a simple procedural exercise. Although the EDPS welcomes decisions to communicate personal data breaches even in the absence of a high risk, the content of such communications frequently failed to adequately reflect the requirements set out under Article 34(3)(b), (c), and (d) of Regulation (EU) 2018/1725. As a result, the core objective of the transparency principle established by the regulation was not fully achieved. Effective communication with data subjects following a personal data breach must provide clear, complete and honest information, as this is essential to enable affected individuals to understand the situation, receive appropriate guidance and take necessary measures to protect themselves.

5.4.7. Inadmissible data breach notifications

We also received four requests for support from EUIs to assess the admissibility of a potential breach. These requests were qualified either as posing unlikely risk to individuals' cases, or as not meeting the legal definition of personal data breach. We also received five notifications sent from private companies or individuals (whistleblowers), which were outside the scope of the EDPS's legal competence. These cases involved companies with their main establishment in the EU, in which case the corresponding EU national DPA under GDPR would be competent. Other notifications falling under this category were from companies processing data of EU citizens without an establishment in the EU. EDPS provides to such non-EUI organisations the necessary legal information to re-direct their requests in an appropriate and compliant manner.

5.5. Cybersecurity regulation

Since 2024, EUIs have been required to follow not just the EU's data protection rules for EUIs (Regulation (EU) 2018/1725) but also a new Cybersecurity Regulation, along with guidelines from the cybersecurity supervisory authority – the Inter-Institutional Cybersecurity Board (IICB). The regulation aims to establish a high common level of cybersecurity across EUIs and reduce risks in digital environments.

Apart from these new compliance obligations, under the regulation, the EDPS now serves as a permanent member of the IICB, tasked with contributing its expertise in data protection and privacy. In this context, the EDPS participated in IICB regular meetings, and contributed to proposed guidelines and other deliverables.

As an EUI subject to the Cybersecurity Regulation, in 2025 the EDPS submitted four deliverables to the IICB:

(i) an 'initial cybersecurity review' to spot major weaknesses, accompanied by

(ii) the 'initial cybersecurity plan' with short-term actions to quickly boost the EDPS defences based on the results of the initial review;

(iii) the Cybersecurity Maturity Assessment based on the maturity methodology provided by CERT-EU, together with

(iv) the Cybersecurity Risk Assessment, taking into account the results of the other three deliverables.

These four deliverables will provide the basis for the EDPS Cybersecurity Plan, to be submitted to the IICB in January 2026, according to Article 9 of the Regulation. This deliverable will further augment the 'initial cybersecurity plan' with concrete actions to materialise a minimum maturity level (level 1).

CHAPTER SIX

ARTIFICIAL INTELLIGENCE

Since 2024, the European Data Protection Supervisor (EDPS) has been entrusted with a new, additional mandate stemming from Regulation (EU) 2024/1689, also known as the Artificial Intelligence (AI) Act. The AI Act designates the EDPS as the market surveillance authority (MSA) for AI systems put into service or used by European Union institutions, bodies, offices and agencies (EUIs).

The AI Act also designates the EDPS as a notified body with relation to certain "high-risk" AI systems intended to be put into service by EUIs. This means the EDPS is responsible for testing, certifying and inspecting these systems to ensure they meet the applicable requirements.

6.1. Preparedness for supervision and enforcement

In view of the August 2026 deadline regarding the entry into force of high-risk AI provisions under the AI Act, the EDPS intensified its preparations to act in its role as MSA and notified body. In 2025, we focused on establishing the following organisational, analytical and procedural foundations for effective supervision of AI systems across the EU public administration.

6.1.1. Consolidating the AI Unit

A key priority in 2025 was the consolidation of our AI Unit, bringing together legal, technical and policy expertise to move from strategic preparation to concrete supervisory action. We carried out technical and procedural preparatory steps and invested in technical and human expertise to ensure that the EDPS keeps pace with a fast-evolving AI landscape.

We continued building dedicated institutional capacity in AI technologies, data and data computing, health and safety risks, and knowledge of existing standards and legal requirements, as per Article 70(3) of the AI Act.

6.1.2. Mapping

To supervise AI effectively, it is essential to understand how it is already used in practice across EUIs. Therefore, we carried out a mapping exercise to identify the AI systems currently in use, as well as those planned for future deployment. The results of this exercise were published in a dedicated report.

Through this mapping, we observed that EUIs are more often users than developers of AI systems. Most institutions rely on externally developed, off-the-shelf tools. This finding confirms the importance of ensuring that EUIs remain accountable for how AI systems are deployed and used, even when these systems are procured from third parties.

We also noted the growing presence of generative AI tools, reflecting broader technological developments. At the same time, many AI systems reported by EUIs were still in pilot or development phases. This shows that EU public administration is actively exploring AI, while progressively building internal experience and governance structures.

Finally, we identified that AI systems with a potentially higher impact on individuals are more likely to be used in sensitive policy areas, such as migration, law enforcement and employment. By providing greater clarity on where such systems may emerge, the mapping helped to demystify the concept of "high-risk" AI and to underline that these systems are not prohibited, but require strong governance and oversight.

6.1.3. Developing internal procedures

Building on the insights gained from the mapping exercise and our legal analysis, the work transitioned into a new phase, focused on translating knowledge into operational readiness for supervision under the AI Act. In other words, we moved from understanding how AI is used in EUIs to preparing for hands-on supervision of these systems.

To prepare to use MSA powers under the AI Act, including measures pursuant to Regulation (EU) 2019/1020 (the Market Surveillance Regulation), the AI Unit began developing its internal procedures and making adjustments to its organisational structure. The procedural changes are aimed at ensuring non-discriminatory, transparent, and independent operationalisation of the EDPS's new role, and at creating a coherent supervisory framework for AI systems developed or deployed by the EUIs, providing legal certainty and reducing the risk of compliance gaps.

In particular, the AI Unit worked towards establishing functional separation between the EDPS's responsibilities as a data protection authority under Regulation (EU) 2018/1725 (the data protection regulation for EUIs) and the EDPS's responsibilities as an MSA and notified body under the AI Act. This distinction is crucial for oversight and coordination, for efficient cooperation with the authorities protecting fundamental rights, and for the clear definition of the enforcement procedures, including those on complaints handling.

The AI Unit also closely followed the development of harmonised standards under the AI Act. These standards will be key to translating legal requirements into concrete technical and practical operations. By anticipating how standards are likely to shape compliance expectations, we will be able to support EUIs, provide clear guidance and reduce uncertainty during the AI Act implementation phase.

6.2. Institutional empowerment

In 2025, we continued to focus on institutional empowerment, ensuring that EUIs are not only aware of their obligations under the AI Act, but also equipped with the knowledge, tools and networks needed to implement them in practice. Two main initiatives were developed to fulfil this function: (1) the AI Act Correspondent Network and (2) the AI regulatory sandbox pilot project.

6.2.1. Advancing the AI Act Correspondent Network

The central pillar of our institutional empowerment work was the ongoing development of the AI Act Correspondent Network (AIACN). The network was established by the EDPS in 2024, drawing inspiration from international governance structures and building on the successful experience of the DPO network. Each EUI has voluntarily appointed representatives with different backgrounds and expertise (technical, legal, etc.) to participate in its meetings and activities.

The AIACN serves as a hub for compliance support, capacity-building and knowledge exchange on AI governance. In 2025, it also played the role of a forum for sharing best practices, coordination and mutual learning among EUIs as they prepare for the AI Act.

In 2025, we organised two meetings of the AIACN in Brussels, bringing together correspondents from across EUIs. The first official meeting, in January 2025, focused on setting the foundations for AI preparedness across EUIs. We provided an overview of the AI Act timeline and ongoing work at EU level, clarified key roles under the AI Act, and discussed when and how supervisory authorities come into the picture.

The second meeting, in October 2025, built on this initial groundwork. First, the keynote speaker of the event addressed the audience with considerations regarding the fundamental rights impact assessments in relation to AI governance. Then, the European Commission's AI Office delivered updated guidance on the implementation of AI Act provisions relevant for EUIs. Finally, the EDPS shared preliminary findings from its mapping of AI systems used by EUIs, allowing participants to situate their own practices within a broader administrative landscape.

6.2.2. Launching the AI regulatory sandbox pilot project

As part of our efforts to support EUIs in preparing for the AI Act, and in the context of the Second Meeting of the AI Act Correspondents Network, we launched a pilot project to establish an AI regulatory sandbox. This initiative responds to the need to reconcile innovation with compliance at a time when many EUIs are developing or deploying AI systems, often in conditions of legal and technical uncertainty.

The sandbox pilot project is conceived as a controlled testing environment in which EUIs can develop, test and validate AI systems before deployment. Within this framework, we aim to provide tailored regulatory guidance, while ensuring that fundamental rights and safety requirements are respected. By allowing AI systems to be tested under defined conditions and with the guidance of the regulator, the sandbox should help EUIs in identifying and addressing potential compliance challenges early in the development process, reducing the risk of costly adjustments once systems are operational.

The pilot approach reflects the current regulatory context. Our enforcement powers under the AI Act will apply from August 2026, together with the provisions regarding regulatory sandboxes. Ahead of this date, the pilot project will provide a cooperative space for experimentation and mutual learning, and will enable EUIs to reflect on concrete AI use cases.

At the same time, it will support the EDPS in better understanding institutional needs and implementation challenges, in view of the possible establishment of an official regulatory sandbox.

Participation in the pilot project is voluntary and reflects an opportunity rather than an obligation for EUIs.

6.3. Legislative and policy analysis

We played an active role in shaping the interpretation and application of the AI Act within the EU public sector, including the development of key framework documents supporting its implementation. Our legislative and policy analysis focused on ensuring that the regulation is amended and translated into guidance and processes in a way that is legally sound, operationally feasible and aligned with fundamental rights and product safety requirements.

6.3.1. AI Board

The EDPS participates as observer in the AI Board, an advisory and coordination body established by the AI Act to ensure consistent implementation, application and enforcement of the AI Act across EU Member States.

In this role, the EDPS actively attended meetings of the AI Board and several of its subgroups for the purpose of examining specific AI-related issues (e.g. the subgroup on standards, on high-risk AI systems, on prohibitions, and on law enforcement). We contributed to discussions on key aspects of the AI Act's implementation and provided input to public consultations, working groups and background documents prepared within the AI Board framework.

This activity allowed us to:

- highlight within the AI Board the specificities of the EDPS' role in the context of the AI Governance structure set out by the AI Act;
- to consequently share the knowledge acquired through the AI Board meetings with the EUIs to facilitate their timely compliance with the AI Act.

Through our involvement, we supported a consistent and coherent interpretation of the AI Act and helped anticipate future guidance and standards, enabling us to prepare our own supervisory approach and support EUIs early.

6.3.2. Analysing the AI Act

We carried out extensive legal analysis of the provisions of the AI Act, with a particular focus on their application to EUIs. This analysis examined how the AI Act interacts with other legal frameworks, such as the data protection rules and the legal frameworks specific to EUIs. By analysing the AI Act early and in depth, we aimed to anticipate interpretative challenges and contribute to legal certainty for EUIs as they prepare for compliance.

This work also identified practical implications for the functioning of the EDPS itself. This process should ensure that our organisational setup and procedures are aligned with the legal framework.

Overall, our legislative and policy analysis helped bridge the gap between the legal framework and its practical application. It supported participation in EU-level governance structures, strengthened the EDPS's preparedness for its new role, and laid the groundwork for consistent, proportionate and effective supervision of AI systems used within the EU public sector.

6.3.3. Cooperation with MSAs

We strengthened cooperation with national MSAs on issues related to market surveillance, in particular through the participation as full member in the standing sub-group for market surveillance of the AI Board (which acts as the administrative cooperation group for the AI Act). This engagement was essential in 2025

to ensure consistent supervision and information-sharing between MSAs, in support of coherent application of the AI Act and to avoid fragmented oversight.

6.4. International engagement and exchange of best practices

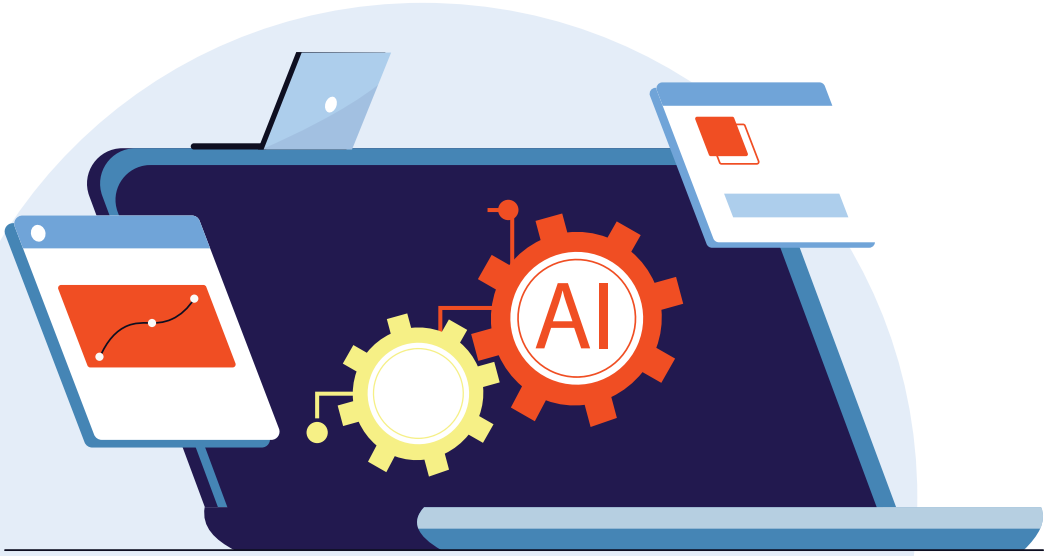
Recognising that AI governance challenges are inherently cross-border, the EDPS, in its role as MSA and notified body, ensured its presence in international institutions, networks and organisations working on AI matters, and contributed with its expertise and know-how to the sharing of best supervisory and enforcement practices.

We participated in international organisations and gatherings with relevant stakeholders outside of the EU/EEA, inter alia, contributing to the work of:

- the Global Network of AI Supervisory Authorities (GNAIS), led by UNESCO (United Nations Educational, Scientific and Cultural Organization), as a full member, working with other supervisors on assessment frameworks, methodologies and supervisory tools;
- the Council of Europe, including on the development of the methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (HUDERIA methodology);
- the activities and meetings organised by the Organisation for Economic Co-operation and Development's Artificial Intelligence Policy Observatory (OECD.AI) and its Global Partnership on Artificial Intelligence (GPAI).

We also engaged with research initiatives which support evidence-based policymaking and strengthen links between research and supervision. An example of one such initiative was the NoLeFa project, which brings together public bodies, small-and-medium enterprises (SMEs), startups, and an EU research network to promote safe and trustworthy AI by supporting market surveillance with testing, coordination and standardisation efforts.

Additionally, the AI Unit shared expertise through active EDPS engagement as a speaker at international events and strengthened collaborations on AI matters with independent technical experts and academia.



CHAPTER SEVEN

INFORMATION AND COMMUNICATION

As an organisation, the European Data Protection Supervisor (EDPS), places strong emphasis on communicating our activities in a transparent and accessible manner. We aim to explain clearly, in language that is accessible to a broad audience, what we do and why we do it. Effective communication is an essential part of ensuring accountability and fostering trust in the EU administration.

Over the years, through the Information and Communication Unit (I&C Unit), we have developed and consolidated a strong online presence, notably through our website and social media channels. These platforms allow us to reach diverse audiences – including EU institutions, stakeholders, practitioners and the wider public – and to tailor our messages according to the nature and complexity of the information provided.

By using a range of communications tools in a coordinated and strategic manner, we seek not only to inform the public about data protection and AI matters, but also to enhance the visibility, clarity and impact of our work.

7.1. EDPS's online presence

In 2025, we continued to strengthen and diversify our digital footprint to ensure that our core messages on data protection and AI reach a broad and diverse audience. With this aim, we have built and continue to expand a strong online presence across our core social media channels – X, LinkedIn and Instagram – including through the organisation of regular and targeted social media campaigns. We also reactivated our presence on Mastodon, further broadening the range of platforms through which stakeholders can engage with our work. At the same time, we use the EDPS website as our main communications hub, providing comprehensive information on our priorities, activities and key developments.

7.1.1. Social media channels

Social media has increasingly become a key communications tool. Throughout 2025, we maintained an active and transparent presence across various platforms, including X, LinkedIn, YouTube, Instagram and more recently Mastodon, allowing us to reach a global audience quickly and effectively.

By the end of 2025, the total number of our followers across all platforms exceeded 129,000, which reflects the increasing public interest in data protection and privacy.

Our account on X enabled us to highlight the EDPS's participation in a wide range of events and to share the key messages and objectives of our work.

LinkedIn remains our primary social media channel to promote our institutional communication, to engage with professionals and to strengthen our employer brand, enabling us to connect with a highly specialised audience of privacy, data protection and AI professionals, institutional stakeholders, and prospective candidates.

In 2025, alongside our regular daily activities, we implemented several targeted thematic campaigns aimed at raising awareness of our mandate, showcasing our expertise, and highlighting career opportunities within the organisation.

The impact of these efforts is reflected not only in the steady growth of our follower base, but also in the high levels of engagement generated by our content. LinkedIn continues to be our fastest-growing platform, confirming its strategic importance in reaching and mobilising our core audiences.

Our YouTube channel provides a platform to share footage from events, publish awareness-raising videos, and broadcast some of the Supervisor's most important speeches. In 2025, we used the channel to promote EDPS video podcasts, a series of videos entitled 'Meet #teamEDPS' showcasing our colleagues, and other content highlighting our activities and priorities. The steady growth of our audience on YouTube reflects the increasing role of video as an effective communications tool.

The EDPS Instagram account, since its launch in February 2024, has shown steady and sustained growth. The platform features engaging, educational, and interactive content – including short videos, carousels, vibrant images and reels – designed to reach a youthful audience with a basic understanding of data protection. Through this content, we aim to show how privacy and the digital landscape relate to everyday life, making data protection more accessible and relevant.

In 2025, we reactivated the EDPS Mastodon account, previously operating as EU Voice, which had been closed in May 2024 following the conclusion of its pilot phase. This initiative aimed to reintroduce an alternative communications tool in support of a more democratic, decentralised and privacy-friendly model of social media. On Mastodon, we share updates on the activities of the Supervisor and provide a window into our daily work, offering followers a relatable and transparent view of our ongoing efforts in data protection and privacy.

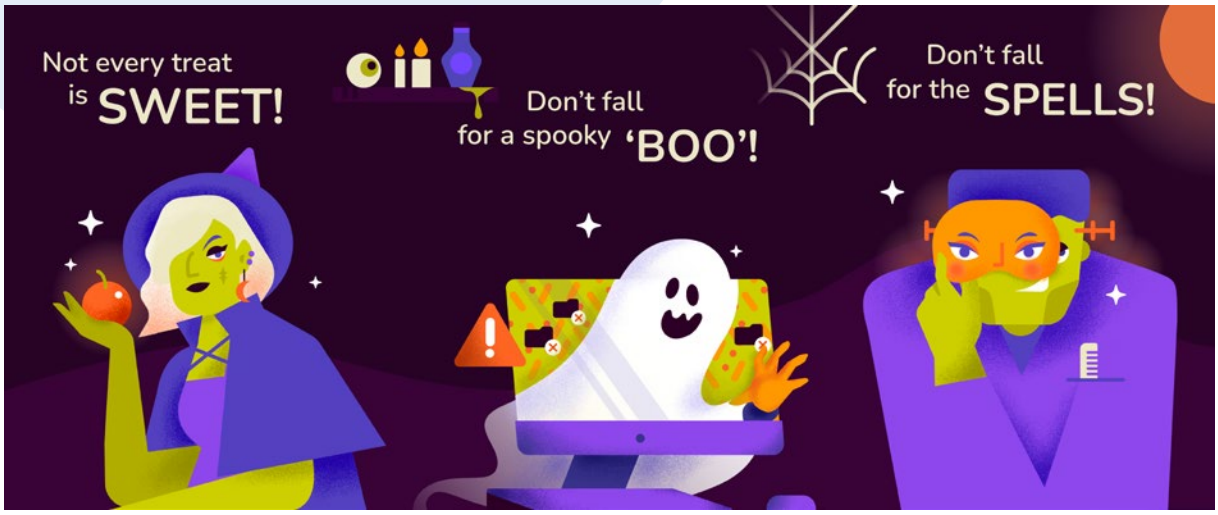
7.1.2. Social media campaigns

Throughout 2025, we used our social media channels strategically to design and implement a range of targeted campaigns aimed at increasing our outreach and keeping our audience informed about our work. Some campaigns focused on promoting upcoming initiatives and events, while others highlighted key publications or milestones to ensure that important messages reached a wider audience. In addition, social media played an integral part of broader communication efforts, helping us amplify our priorities across multiple platforms in a coherent and coordinated manner.

#InCaseYouMissedIt

As our social media community continues to grow, we run the #InCaseYouMissedIt campaign twice a year across our platforms. This initiative highlights important but less high-profile topics and brings renewed attention to key activities that our audience may have missed over the past months.

European Cybersecurity Month



In October 2025, we marked the 13th edition of European Cybersecurity Month (ECSM). To celebrate the occasion, we launched a dedicated social media campaign focusing on the human element in cybersecurity, the central theme of this year's ECSM.

The campaign promoted a podcast episode on human oversight of automated decision-making which explored how the use of automation is expanding in sectors such as healthcare, finance, defence, transportation and public administration, creating new opportunities while also posing challenges for privacy and data protection. It also featured a series of thematic factsheets designed to raise awareness and foster informed discussion on cyber threats. By engaging with a broader audience through these initiatives, we continue to advocate for responsible deployment of AI and strengthening cyber resilience across EU institutions.

Monthly recap

Throughout 2025, we also kept our audience regularly informed of our work through periodic posts across our social media channels. We highlighted our opinions, guidance and other key documents to ensure that important developments did not go unnoticed. This consistent visibility is essential in a fast-moving digital environment, where significant publications can easily be overlooked. By revisiting

and explaining our work in an accessible format, we help stakeholders stay informed, support transparency, and encourage broader understanding of data protection issues within the EU administration and beyond.

Myths busted

This campaign addressed common misconceptions about data protection and privacy. We aimed to clarify misunderstandings, provide accurate information and empower citizens to better understand their rights to data protection in the digital environment. We continue making these topics more accessible, relatable and easier to navigate for both the general public and professionals.

7.1.3. EDPS website

The EDPS website remains our primary communications channel and the central hub for our activities. It hosts our latest news, press releases, newsletters, podcasts and videos, alongside our core legal publications, including opinions and formal comments, to name a few. Ensuring that the website is user-friendly and accessible remains a key priority. We therefore continuously enhance its features and design in response to users' feedback and evolving needs. In 2025, this commitment was supported by several technical improvements aimed at strengthening functionality, accessibility and overall user experience.

7.2. Engaging beyond headlines

Data protection is no longer a niche topic reserved for specialists. It increasingly shapes everyday life in a rapidly evolving digital landscape, particularly with the growing mainstream use of artificial intelligence (AI). As public interest continues to expand, so too does the need for accessible, reliable and insightful information.

To respond to this demand, we further diversified and strengthened our communication formats in 2025. We enhanced our newsletter, continued to develop our podcast channel, and expanded our blog with exclusive insights into the international activities of the Supervisor and the Secretary-General. Through these channels, we bring our work closer to stakeholders and the wider public, offering deeper context and sustained engagement beyond individual announcements.

7.2.1. EDPS Newsletter

The EDPS Newsletter remains a popular and accessible communication tool, designed for both mobile and desktop users. Counting 9,014 subscribers, it helps us reach audiences with varying levels of expertise in data protection.

In 2025, we published five editions which provided concise updates on our work. Each issue covered a broad range of topics, from technology monitoring and key opinions and formal comments, to supervisory and enforcement activities, and events organised or attended by the EDPS. Particular attention was given to emerging technological trends, notably AI, digital identity and automated decision-making, as well as international data transfers and evolving compliance challenges. We also maintained our EDPS Tips & Tricks section, offering practical guidance for protecting personal data in everyday life.

Together, these newsletters ensure our work remains transparent, informative and accessible to a wide audience.

7.2.2. Podcasts – updates on the go

Our podcast channel, 'EDPS on Air', continued to expand its audience in 2025. Launched in December 2022, it brings listeners closer to our work in a concise and engaging format, with most episodes lasting under ten minutes.

The channel is structured around two distinct series:

- **Newsletter Digest** – This series provides updates on the EDPS's activities and complements our newsletter, reaching different audience groups. Occasionally, we also invite guests from the data protection field to share their perspectives and offer additional in-depth and insight.
- **TechDispatch Talks** – Produced in collaboration with the EDPS's Technology and Privacy Unit, TechDispatch Talks explore the intersection of technology, privacy, and data protection, with a focus on emerging trends. In 2025, episodes covered topics such as Human Oversight of Automated Decision-Making, examining the societal and privacy implications of technological advances from mechanised production lines to modern autonomous systems, and Federated Learning, showcasing a collaborative and privacy-friendly approach to AI model training.

All episodes are available on the 'EDPS on Air' channel on our website, through our Podcast RSS Feed, and can also be accessed on Spotify, broadening our reach and accessibility. Across both series, we strive to produce informative and engaging content that appeals to all audiences interested in data protection.

7.2.3. EDPS blog – sharing a personal perspective on privacy and data protection

The EDPS blog offers a space for the Supervisor, Wojciech Wiewiórowski, the Secretary-General, and occasionally Heads of Units, to share personal reflections, and updates on their activities, as well as on the broader work of the EDPS.

The blog is prominently featured on the homepage of our main website, where a short excerpt from the latest post is always visible. In 2025, we published thirteen blogposts covering a wide range of topics, providing readers with accessible and engaging commentary on key developments in data protection and privacy.

Our posts highlighted meetings of the AI Act Correspondents Network and DPO network, major events such as CPDP Data Protection Day 2025 and Schuman Day, as well as strategic publications, including the Concept Note on a Digital Clearinghouse 2.0, among others.

7.3. Public relations – keeping stakeholders informed

Engaging with the media and responding to public inquiries allows us to ensure transparency, raise awareness of our work, and keep citizens informed about key developments in data protection, privacy and AI. Through press releases, interviews and press events, we communicate our activities, positions and priorities in a clear and accessible way.

7.3.1. Press releases and media relations

Press releases are a key tool for informing journalists and other stakeholders about significant developments in data protection and the EDPS's work. They highlight our contributions to shaping policy and practice, including opinions on proposed regulations, enforcement actions and key reports.

In 2025, the EDPS issued 12 press releases, all of which are available on our website. These communications covered our most impactful activities, including the EDPS reprimand for the European Border and Coast Guard Agency (Frontex), our participation in the fourth Coordinated Enforcement Action, the European Commission's compliance with Regulation (EU) 2018/1725 (the Data Protection Regulation for EUIs) in relation to its use of Microsoft 365, and the publication of EDPS Guidance on Generative AI, among others.

Our media engagement goes beyond press releases. We also organise press conferences and in-person interviews, providing the Supervisor with the opportunity to communicate directly with the press – an essential channel to ensure accurate and timely coverage of our work. In addition, we handle written press inquiries, which remain an important means of keeping the public informed about the EDPS's activities and positions.

7.3.2. Public requests

In 2025, we continued to receive public requests for information from individuals eager to learn more about our work, our powers, and their rights regarding personal data. Requests are mostly submitted in English, German or French, and we always reply in the same language, provided it is one of the EU's official languages. This approach allows us to provide timely and accurate information to EU citizens and other nationals, while ensuring our work is transparent and accessible to a wide range of stakeholders. For requests that fall outside our direct competence, we guide the requester to the appropriate authority or organisation, either within or outside the European Union.

7.3.3. Events

Events and direct engagement with stakeholders and audiences play a key role in fostering meaningful dialogue, strengthening trust, and ensuring clear and impactful communication.

In 2025, the EDPS actively contributed to the organisation, logistical coordination and promotion of several key initiatives. In a number of cases, we worked closely with co-organisers contributing to programme development, shaping the visual identity and supporting the overall delivery. These engagements provided valuable platforms for discussion, knowledge exchange and policy reflection in the field of data protection and privacy. Key events in 2025:

CPDP – Data Protection Day: A new mandate for data protection

On 28 January 2025, together with the Council of Europe (CoE) and CPDP Conferences, we celebrated Data Protection Day with a special edition of CPDP entitled 'Data Protection Day: A new mandate for data protection'. This one-day event focused on the evolving mandate of data protection, particularly its essential role as a safeguard of democratic society against excessive intrusions into citizens' privacy by public and private actors. The event attracted significant interest, with 500 in-person attendees and more than 2,000 online connections throughout the day.

EU Open Day 2025

Every year in May, we celebrate Europe Day, commemorating the Schuman Declaration, which laid the foundations for peace and unity in Europe. On 10 May 2025, the European institutions opened their doors to the public, providing an excellent opportunity to engage citizens and raise awareness of their data protection and privacy rights.

Together with the European Data Protection Board (EDPB), we participated in the celebrations with an exhibition stand featuring interactive activities for all ages. Visitors could learn about our work and its relevance, explore our AI-based deep fake generator, and test their knowledge through our Data Protection Quizzes.

CPDP – Computers, Privacy and Data Protection conference 2025

CPDP.ai 2025
18th international conference
21-23 May ▪ Brussels, Belgium
THE WORLD IS WATCHING

Following tradition, the EDPS participated in the annual CPDP conference on privacy and data protection, held in Brussels from 21-23 May. The conference serves as a key forum for discussing the intersection of privacy, technology and digital governance.

In 2025, we organised two dedicated panels, on AI and on data protection. In addition, many of our experts contributed as speakers in other sessions, we hosted an exhibition booth, and the Supervisor delivered, as in previous editions, the conference's closing remarks.

High-Level Debate on Competition, Innovation and Data Protection

On 3 June 2025, the EDPS, the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) and the Bavarian Data Protection Commissioner (BayLfD) co-organised a high-level debate to reflect on recent developments relating to the EU's Digital Rulebook.

The event, kindly hosted by the Representation of the Free State of Bavaria to the EU, provided an excellent forum for digital regulators to discuss cooperation on effective protection of citizens, fostering innovation, and supporting the Union's competitiveness.

PATRICIA II – Personal dATa bReach awareness in Cybersecurity Incident hAndling

On 5 June 2025, the EDPS organised the second edition of PATRICIA (Personal dATa bReach awareness In Cybersecurity Incident hAndling), a tabletop exercise focused on personal data breach management. The exercise brought together key stakeholders from selected EU institutions, including IT personnel, Data Protection Officers and Security Officers, to enhance incident response and collaboration.

PATRICIA provides a practical platform to strengthen awareness of personal data breaches and improves risk mitigation across the EUIs. This edition involved seven teams engaging in an evolving cyberattack scenario, exchanging best practices, testing response mechanisms and refining coordination strategies.

In 2025, the EDPS was awarded at the Global Privacy Assembly (GPA) Awards in the Accountability category for this strategic initiative to enhance personal data breach management across EU institutions. This recognition highlights the value of initiatives where supervisory authorities build capacity, foster collaboration, and promote continuous improvement in data protection.

From Cradle to Cloud: Surveillance and Digitalisation around Childhood

On 4 July 2025, the EDPS and the EDPB Trainees organised the conference 'From Cradle to Cloud: Surveillance and Digitalisation around Childhood', focusing on the digital rights of minors. The event brought together stakeholders in data protection and children's rights to explore how technological developments, from AI-powered toys to social media and personalised learning tools, affect children's privacy and digital footprint.

Participants discussed regulatory frameworks, best practices, and strategies to foster privacy compliance and literacy in educational and online environments. The conference also provided a platform for young professionals in the institutions to apply their knowledge, gain practical experience, and engage in timely discussions on current data protection challenges.

International Organisations Workshop on Data Protection 2025

On 25-26 September 2025, the EDPS and UNESCO (United Nations Educational, Scientific and Cultural Organization) co-hosted the 20th edition of the International Organisations Workshop (IOW) on Data Protection at UNESCO headquarters in Paris, with a hybrid format allowing online participation. The workshop brought together 180 representatives from 86 international organisations to exchange insights on safeguarding privileges and immunities, independence, digital sovereignty and personal data in a rapidly evolving geopolitical context.

The event featured high-level panels, sessions on AI and international data transfers, and practical workshops on anonymisation, IT compliance, risk management, Data Protection Impact Assessments, and handling data subject requests. The hybrid format and breakout sessions enabled deeper engagement and knowledge sharing, providing a unique platform for participants to discuss challenges, best practices and updates in data protection across international organisations.

7.3.4. The value of study visits: strengthening knowledge and dialogue

Study visits remain an integral component of our communication and outreach efforts, providing a direct and meaningful way to engage with stakeholders. Through this initiative, we raise awareness of the EDPS's mandate, powers and day-to-day work, while promoting a deeper understanding of the fundamental rights to privacy, data protection and AI supervision.

These visits are primarily addressed to small groups, including specialised university students, representatives of national and local administrations, and other interested stakeholders from across the EU and beyond. They offer participants the opportunity to engage directly with EDPS staff, ask questions and gain practical insight into how data protection and AI are applied within the EU institutional framework.

In 2025, we organised nine study visits, bringing together 194 participants – an increase compared to 2024. While most visits took place at our headquarters in Brussels, one session was hosted at our Strasbourg office, further broadening our institutional outreach.

7.4. Employer branding – careers with purpose

As a growing institution, the EDPS must not only attract highly qualified professionals, but also retain them and foster an environment in which they can thrive.

In 2025, we continued to invest in our employer branding efforts, further strengthening the EDPS's visibility as an employer and consolidating its reputation as an attractive and meaningful place to build a career.

To support this objective, we designed and implemented a range of targeted communication activities and campaigns. While the I&C Unit led these initiatives, they were carried out in close cooperation with the EDPS's Human Resources and Budget Administration Unit, ensuring a coherent and strategic approach.

7.4.1. Revamp of the EDPS Careers page

In 2025, the comprehensive overhaul of the EDPS Careers page was a flagship employer branding initiative. The redesigned page offers a more modern and engaging presentation of the organisation, its culture and the career opportunities available within it, while maintaining the visibility of our Staff Ambassadors, who provide authentic insight into life at the EDPS.

The new structure improves navigation and access to key information, offering prospective candidates a clearer and more compelling overview of career opportunities.

7.4.2. #TeamEDPS campaigns

Several dedicated employer branding campaigns were rolled out across our social media channels throughout the year, some running over several weeks to ensure sustained visibility and engagement.

Under the banner '#teamEDPS – Join us', we showcased the distinctive career opportunities offered by the EDPS, positioning the organisation as an employer of choice and driving traffic to our revamped Careers page.

Complementing this initiative, the 'Meet #teamEDPS' campaign featured video testimonials from our Staff Ambassadors, offering authentic insights into daily work at the EDPS, our organisational culture and the professional paths available within our teams.

Targeted campaigns were also conducted to promote the Blue Book Traineeships, with a particular focus on attracting early-career professionals and young talent interested in EU public service and data protection. In parallel, we ensured consistent promotion of newly published vacancy notices, increasing their visibility and supporting timely outreach to qualified candidates.

While LinkedIn remained our primary platform for these initiatives, reflecting its strong professional focus, the campaigns also generated meaningful engagement on Instagram, allowing us to reach a broader and more diverse audience.

CHAPTER EIGHT

HUMAN RESOURCES, BUDGET AND ADMINISTRATION

As an organisation, the EDPS must manage its human and financial resources efficiently to be able to deliver on its mandate and tasks as the data protection authority (DPA) of the EU institutions, bodies, offices and agencies (EUIs).

This chapter highlights on how, through the Human Resources and Budget Administration Unit (HRBA Unit), the EDPS invested in attracting, onboarding and retaining employees, and how it continues to help its employees develop through training and other activities.

It also presents how the EDPS optimised its financial management, procurement and administrative processes in 2025 to ensure efficient resource use and support its expanding responsibilities.

The HRBA Unit carries out these tasks also for the European Data Protection Board (EDPB), for which the EDPS provides the Secretariat.

8.1. Talent attraction, recruitment and onboarding

8.1.1. Employer branding

In 2025, the EDPS employer branding initiative led by the I&C Unit played an important role in attracting and securing the expertise required for the organisation to fulfil its mandate. The HRBA Unit continued to contribute actively to this initiative by ensuring the alignment of all human resources (HR) processes and internal communication across the entire employee lifecycle.

8.1.2. Diversity and inclusion

In 2025, the EDPS began reflecting on a diversity and inclusion strategy which is suitable for its position as a medium-sized organisation. For this purpose, HRBA Unit members participated in formal and informal interinstitutional working groups and gathered good practices from

comparable institutions. Furthermore, a call for expression of interest for an EDPS internal working group on diversity and inclusion was finalised and prepared for launch in early 2026.

8.1.3. Traineeship programme

During 2025, the EDPS continued to participate as a hosting institution in the Blue Book Traineeship programme of the European Commission. The programme allows the EDPS to onboard each year, on 1 March and 1 October, two cohorts of ten Blue Book trainees.

Given the high interest of EDPS and EDPB teams in this programme and the limited number of trainees available, an internal rotation system was established in 2023 allowing all services to benefit from it at regular intervals. The HRBA Unit serves as a contact point for managing the programme internally, offering support to the recruiting units throughout the selection process, and oversees the allocation and distribution of quotas, coordinating logistics and welcoming trainees.

8.1.4. Enhanced recruitment procedures

The EDPS continuously strives to build diverse teams of legal, technical and other relevant experts from across the EU, working together to shape a safer digital future. The EDPS employs staff from 23 Member States, thus representing broad cultural and geographic variety.

In 2025, 19 successful selection procedures were carried out for this purpose, resulting in the recruitment of 5 officials, 13 contract agents and 1 temporary agent. Besides the selection procedures, a reserve list of qualified candidates for contract agent positions was established to facilitate future recruitment for vacant positions with corresponding profiles.

All recruitment procedures are centrally managed by the HRBA Unit. Apart from the recruitment of new staff to fill new posts or replace leaving staff, the HRBA Unit also manages short or long-term replacements due to staff absences, for example through interim staff or external consultants.

On behalf of the EDPS, during 2025, HRBA Unit members continued to participate in a joint working group of representatives from all EU institutions dedicated to the topic of recruitment. The working group creates an important forum to keep abreast of state-of-the-art approaches, share experience, identify opportunities for collaboration, and enhance operational efficiency across EUIs.

Furthermore, with the EU AI Act adopted in 2024, the EDPS received new supervisory tasks. The staffing of the new Artificial Intelligence Unit created for this purpose entailed the need to recruit specialised profiles with demonstrated expertise in artificial intelligence (AI), in order to equip the unit with the technical capacity necessary to fulfil its mandate.

8.1.5. Continuous improvement of onboarding procedures

In 2025, the HRBA Unit invested significantly in improving the onboarding procedure for newcomers. As part of these efforts, the administrative steps for the pre-recruitment procedure were simplified to create a more efficient and integrated workflow. Moreover, the HRBA Unit started to explore the integration of different automated IT tools to optimise the workflow for newcomer onboarding and reduce delays, error rates and administrative burden, with a view to deploying these tools in 2026.

In 2025, the HRBA Unit also increased the frequency of onboarding sessions for newcomers: three sessions were organised, covering presentations of the working portfolios of all EDPS and EDPB teams, as well as trainings on relevant administrative tools and procedures. Moreover, an improved e-welcome for newcomers when taking up duties has been put in place to help them orientate from the very beginning and provide them with a contact person for their questions.

8.2. Talent retention, wellbeing and workplace culture

8.2.1. Update on the retention strategy

The EDPS talent retention strategy adopted in January 2025 establishes a framework of short, medium and long-term actions designed to keep and nurture highly skilled staff. Short-term activities included employer branding measures through cross-unit collaboration and the launch of several staff wellbeing initiatives. Medium-term activities comprised a new legal basis for the employment of temporary agents and the reinforcement of established job shadowing and EDPB secondment programmes. Long-term efforts envisage leveraging insights from the staff satisfaction survey planned for 2026.

8.2.2. Launch of the temporary agent decision

In 2025, the EDPS launched the process for establishing a new legal basis for the employment of temporary agents, next to officials and contract agents. These provisions are expected to be adopted in 2026 and, once in place, they will provide a framework for the recruitment and deployment of temporary agents within the EDPS.

8.2.3. Enhancing HR Services

To ensure that staff has continuous access to relevant HR information and receives tailored support from the HRBA Unit, the unit launched a series of initiatives during the course of 2025. These included the 'HR open doors' initiative which introduced a low-threshold and regular forum for staff to exchange on various topics with HRBA Unit members and to foster an inclusive and efficient work environment. As a complementary measure, the HR intranet section was revamped to provide staff members with comprehensive, up-to-date and easily accessible HR-specific information related to career management, working conditions, learning and development, staff conduct, and wellbeing.

8.2.4. Engaging with the newly elected Staff Committee

The HRBA Unit acted as an intermediary between the EDPS Staff Committee, which was newly elected in 2025, and senior management, by sharing relevant information, providing advice on relevant topics and facilitating an effective collaboration for the benefit of all staff members.

8.3. Talent development, teambuilding and organisational resilience

8.3.1. Internal training

In 2025, the EDPS HRBA Unit continued to organise training courses to enhance staff members' skills, such as AI training, AI and Algorithm Auditor Certificate Programmes (which build core skills for AI auditing, governance and regulatory compliance), and customised pleading and public speaking courses.

Staff members were also encouraged to engage in diversified learning activities, including a call for expression of interest in internal facilitator training, enhancing cross-team collaboration and a sense of belonging and purpose. The organisation of internal teambuilding activities, including on the topic of non-violent communication, helped create bonds for collaboration and wellbeing, especially in newly created or evolving teams.

In addition, the HRBA Unit developed guidelines to support units in the organisation of their team events. The guidelines provide a framework for team-building activities while remaining sufficiently flexible for team-specific needs. All EDPS and EDPB teams are encouraged to organise one team-building event

per year. In addition, an away day is organised for the whole institution, with the objective of further enhancing connection and shared purpose across the EDPS.

8.3.2. Supporting staff and managers in times of change

The HRBA Unit supports staff and managers throughout periods of change, including reorganisations and temporary re-assignments due to absences and turnover, by providing guidance and advice. A close coordination with management ensures that changes are implemented in a fair, transparent and people-centred manner, while staff members are supported through individual consultations, practical HR solutions and wellbeing-focused measures. This approach facilitated smooth transitions, maintained trust, and allowed the organisation and its staff to adapt effectively to evolving needs.

8.3.3. Team events

During 2025, a Wellbeing Strategy was developed to provide a guiding framework for a variety of wellbeing-related measures at the EDPS. The HRBA Unit organised several cross-unit initiatives – including a Christmas workshop, daily stretching sessions, language conversation classes, a brown bag lunch session on robust organisations, and a ping-pong competition – which enhanced staff engagement and cross-team interactions. Before the end-of-year break, a solidarity initiative was launched, resulting in the collection of EUR 1,500 for the St. Pierre d'Angles homeless shelter and the donation of 20 shoeboxes for people in need.

8.3.4. EDPGreen working group

Carbon emissions stem from nearly all human activities. The EDPS promotes a positive vision of digitisation paired with a commitment to respect and defend our natural environment and quality of (work)life. In this context, following a call for volunteers launched at the end of 2024, a thematic cross-unit working group of 12 engaged colleagues, called EDPGreen, was established.

The group aims to take a closer look at the organisation's energy consumption, the carbon footprint in its procurement process, and colleagues' means of commuting to and from work. The working group also promotes various activities focused on environmental responsibility to raise individual and collective awareness.

8.4. Optimising our resources for maximum impact

8.4.1. Budget

The EDPS operating budget for 2025 amounted to EUR 26,973,970. (The initial budget of EUR 27,083,875 was amended following a salary update in October 2025 applying to staff of all EU institutions.) This corresponds to an 11% increase compared to the final 2024 budget. The increase is largely due to the new responsibilities entrusted to the EDPS by the EU legislator in the fields of AI and cybersecurity, as well as the operational requirements needed to ensure the protection of fundamental rights relating to data protection and privacy.

8.4.2. Implementing the 2025 Budget efficiently and effectively

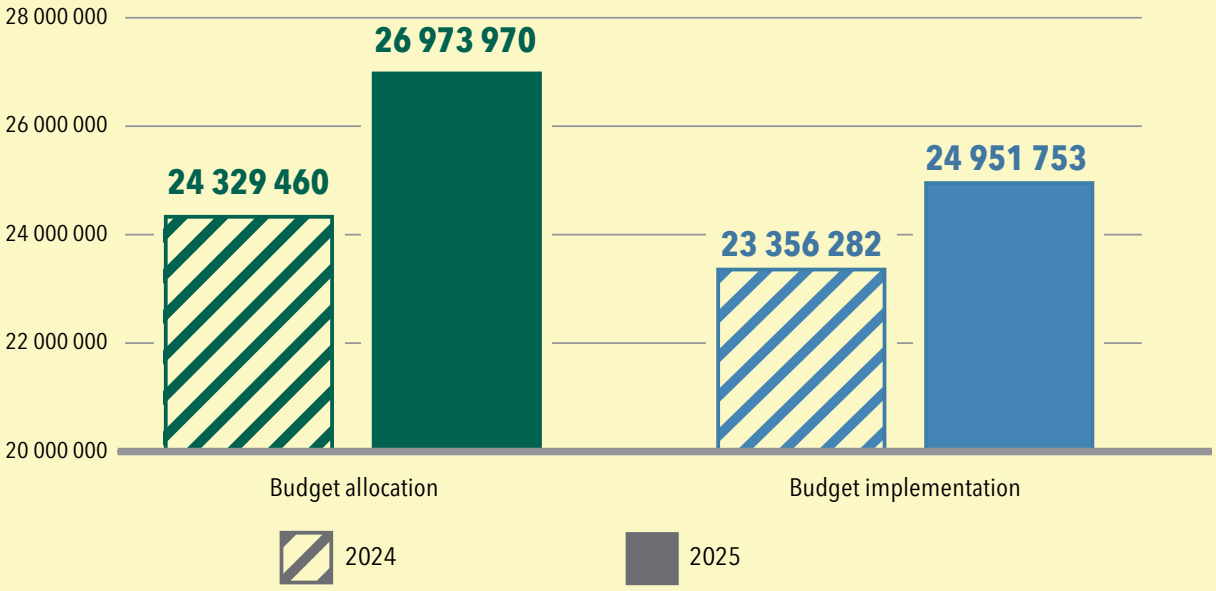
For 2025, the EDPS achieved a remarkable overall budget implementation rate of 92.50%, reflecting rigorous monitoring and sound financial management.

More in detail, staff-related costs (Title 1) reached an implementation rate of 90.35%. Savings were generated due to a slightly-higher-than-expected number of vacant posts and unused credits in relation to the nomination of a new Supervisor.

Building-related expenditure, equipment and other operational costs (Title 2) had an implementation rate of 97.03%, reflecting effective resource allocation and expenditure monitoring.

Expenditure related to the EDPB (Title 3) attained an implementation of 94.10%. Budget lines linked to the contractual obligations of the EDPB with other EU institutions (rent, staff-related administrative costs, financial tools, etc.) increased significantly and required internal reallocations. Savings resulted from the continued use of hybrid and virtual meeting formats for EDPB activities, which helped reduce travel, accommodation, venue rental and catering costs compared to forecasts. Hybrid meetings also enabled broader participation by national DPAs without additional logistical expenses, thereby enhancing operational efficiency.

Graph 16
Budget 2024 v. 2025



8.4.3. Preparing for the 2026 Budget to address future needs

For 2026, the EDPS requested a substantial increase in staff (+26 posts) and appropriations (+27%). This request was proportionate to the growing responsibilities assigned to the institution, particularly under the AI Act, and the rapidly evolving digital regulatory framework.

However, as in previous years, strict budgetary discipline regarding administrative expenditure

and staffing across EU institutions influenced the preparation of the 2026 Draft Budget. Consequently, the European Commission and the Council applied significant cuts, in line with broader savings measures. As a result, the budgetary authorities were not able to agree in full to the EDPS's budget request, granting only 12 additional administrative posts (EU officials), including 5 for the EDPB, and 5 contract agent positions. The final approved budget reflects these changes, with a 13.70% increase in expenditure compared to 2025.

8.5. Finance

8.5.1. Preparing to migrate to a new financial management system

Preparing the onboarding of a new financial management system (SUMMA) in 2026 while ensuring a smooth transition from the system currently in use (ABAC) required a significant allocation of time and human resources during 2025.

The finance team participated in a series of User Acceptance Tests (UATs) throughout 2025, each designed to validate specific test scenarios and business processes within the SUMMA IT environment. Each UAT consisted of one or two days of testing, conducted jointly with the Commission's Directorate-General for Budget (DG BUDG) and other EUIs.

In addition, regular meetings were scheduled to clarify specific points with the different services at the interface of the new system. Furthermore, the EDPS's finance and procurement teams attended targeted training sessions to become hands-on and fully operational.

8.5.2. Performing an increasing number of payment transactions

In 2025, the number of payment transactions reached a new peak at 1,534 – an increase of 6.53% compared to 2024 (1,440). 99.6% of payments were processed on time (within 30 days) and the average payment time was 14.62 days.

As required by Article 74(5) of the EU Financial Regulation, all financial operations are subject to ex ante controls before they are authorised by the Authorising Officer to ensure the correctness of the operation and compliance with the Financial Regulation. These controls comprise the initiation and ex ante verification of an operation for both operational and financial aspects. They are conducted by staff with the required skills after being formally appointed by the Authorising Officer by Delegation.

The EDPS uses checklists with basic controls to be verified by the operational and financial agents involved in the processing of the operations. The use of a dedicated IT tool (Speedwell) facilitates the controls applied on payments and commitments.

Missions, expert payments and salaries are initiated by the Paymaster Office (PMO) of the European Commission in application of the service level agreements concluded between the two institutions. These payments are subject to an additional layer of ex ante controls, which are operated by the PMO in addition to the controls applied by the EDPS.

8.5.3. Co-managing missions and meetings efficiently

Since November 2022, the EDPS has participated in a PMO-led project for shared mission management, ensuring a centralised and consistent approach to reimbursement requests for missions and related expenses. Through a dedicated IT tool for mission management (MIPS+), the PMO verifies supporting documents for compliance with applicable rules, while the HRBA Unit oversees initiation, validation and related information.

In 2024, a new monitoring system for the mission budget was introduced in MIPS+ and continued in 2025, resulting in further cost reductions. This has allowed for a reduction in mission-related expenditure, with the number of missions decreasing by 30% and the average cost per mission falling by 9% during this two-year period.

Table 3
Mission 2024-2025

	2024			2025		
	Number of missions	Average cost	Total costs	Number of missions	Average cost	Total costs
Supervisor	23	€1,698.70	€39,070.05	18	€1,434.92	€25,828.60
EDPS/EDPB Staff	218	€841.76	€183,504.12	206	€757.64	€156,072.81
EDPB Chair	17	€2,503.71	€42,563.00	17	€2,484.47	€42,235.93
EDPB Vice-Chairs	2	€1,179.50	€2,359.00	5	€1,321.37	€6,606.85

In addition to the management of missions and their reimbursement by the PMO, the EDPS also deploys another financial IT tool from the PMO related to the travel and associated costs reimbursement of experts participating in EDPS/EDPB meetings (AGM). In 2025, the total number of financial transactions amounted to 538.

8.6. Procurement

8.6.1. Procuring and contracting complementary services

In 2025, the EDPS and EDPB together launched 47 public procurement procedures, mostly for very low value contracts, as well as 46 purchase orders and specific contracts under Framework Contracts in different areas – such as event organisations, publications, catering, consultancy, IT services, etc. The EDPS participated in 5 interinstitutional tender procedures and launched a second call for manifestations of interest aiming to establish a list of experts for use by the EDPB. As always, throughout the entire public procurement procedure, the EDPS procurement team prioritised an open, fair and transparent selection and competition process, and ensured that external contractors meet high moral and ethical standards. The use of service level agreements and framework contracts also allowed the EDPS to leverage its limited resources.

8.6.2. Simplifying and streamlining procurement procedures

In 2025, a simplification initiative was launched with the objective of establishing clear procedures and general guidelines to support staff involved in procurement-related files. In addition, a review of the task allocation within the procurement team was implemented. Furthermore, to ensure a more efficient collaboration with the operational sides, financial correspondents were appointed in each unit. Due to staff turnover, the full implementation of these changes will be completed during the first semester of 2026.

CHAPTER NINE

GOVERNANCE AND INTERNAL COMPLIANCE

The Governance and Internal Compliance Unit (GIC Unit) of the EDPS, continued to support the institution's work, particularly in the areas of:

- records, archives and knowledge management;
- internal control, risk management and compliance;
- transparency and access to documents.

In 2025, the GIC Unit also facilitated the EDPS's internal compliance with obligations stemming from the AI Act.

9.1. Information, knowledge and internal control management

In 2025, the EDPS published a records and archives management decision that aligns with existing regulatory frameworks but also modernises its approach to information management.

In addition, this year we implemented Service Now, an IT tool to manage incidents and provide user support for the two records management systems the EDPS uses: Case Management System (CMS) for core business activities and Advanced Records System (ARES) for administrative activities.

We also continued appraising our physical archives to ensure the proper application of retention periods and preparations for the EDPS's historical archives, in compliance with the applicable regulations on the EU institutions historical archives.

Regarding knowledge management activities, we continued supporting the EDPS's decision-making process and effectiveness by preparing procedures, guidance and tools for gathering and sharing knowledge.

Throughout the year, we carried out internal control and risk management activities covering key components of the EDPS's internal control environment:

- coordinating audits carried out on selected EDPS processes;
- coordinating the annual risk management exercise and ensuring its follow-up;
- monitoring and reporting on related processes;
- overseeing quality management activities.

In addition, we further supported the institution coordinating the annual budgetary discharge procedure.

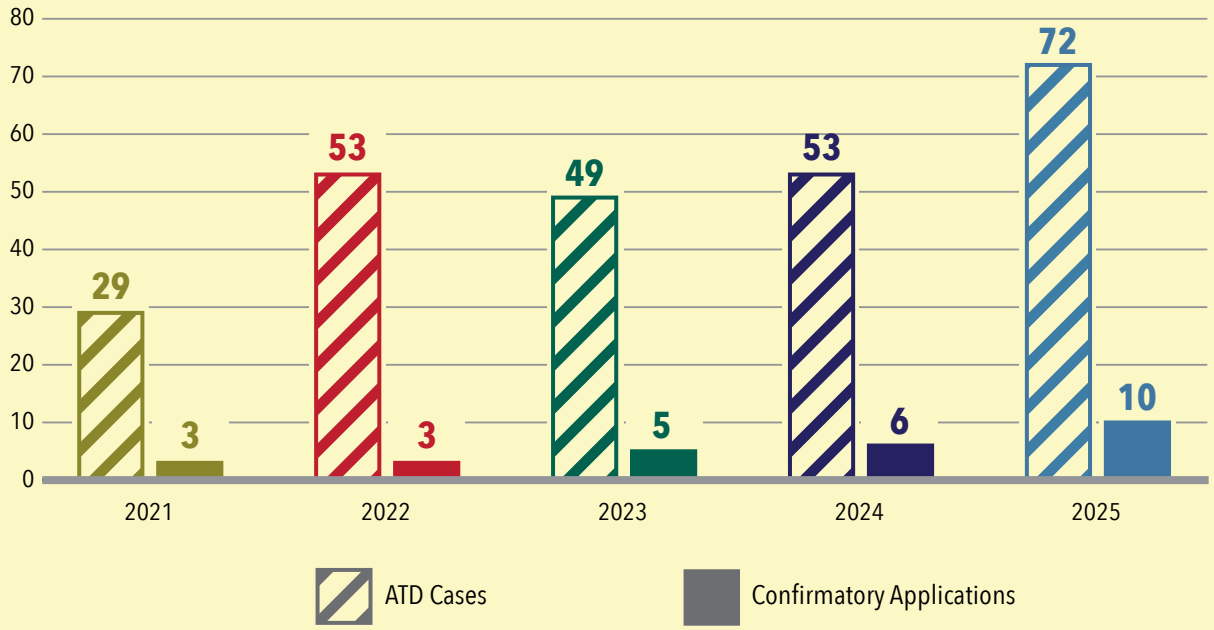
9.2. Transparency and access to documents

As an EUI, and according to the EDPS Rules of Procedure, the organisation is subject to Regulation (EC) 1049/2001 on the public access to documents.

For each request submitted to the EDPS, the Transparency Officer cooperates with the relevant services to respond appropriately to the request.

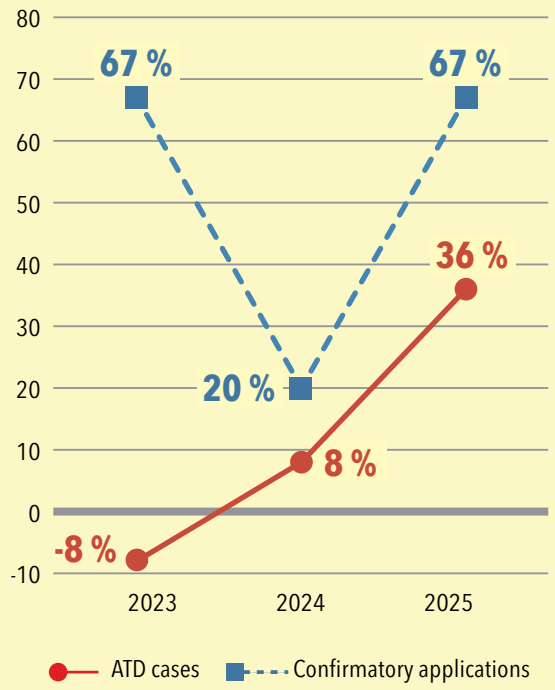
In 2025, the EDPS received 72 access to documents requests, which represents a 36% increase compared to the previous record of 53 cases set in 2024.

Graph 17
Access to documents cases (2021–2025)



In ten of these cases (14% of all 2025 cases), confirmatory applications (appeals) were also received. The number of confirmatory application cases increased by 67% compared to 2024.

Graph 18
Access to documents case dynamics (2023–2025)



Following up on the European Parliament's recommendations in the context of the EDPS's discharge procedures, and in line with its continued commitment to transparency, the EDPS adopted in April 2025 a new set of transparency rules governing interactions with third parties. Under this decision, the Supervisor, the Head of the EDPS Secretariat, and staff with management responsibilities may hold meetings only with interest representatives who are registered in the Transparency Register. Information about these meetings will be made publicly available on the EDPS website. The Transparency Rules are published on the EDPS website and referenced on the website of the Inter-Institutional Transparency Register.

9.3. Internal compliance with AI obligations

In order to facilitate the EDPS's compliance with the obligations stemming from the AI Act, the EDPS appointed an AI Act Correspondent (AIC) who is part of the GIC Unit. The AIC is the contact point of the EDPS as an EU body towards the EDPS in its role as a competent authority and market surveillance authority (MSA) under the AI Act.

In 2025, the AIC facilitated the adoption of the Acceptable Use Policy for publicly available Generative AI systems to be complied with by EDPS staff when using these tools for work-related purposes. It highlights AI systems' inherent limitations and risks and comprises the rules that the EDPS staff must take into consideration and comply with when using such tools, in order to mitigate those risks.

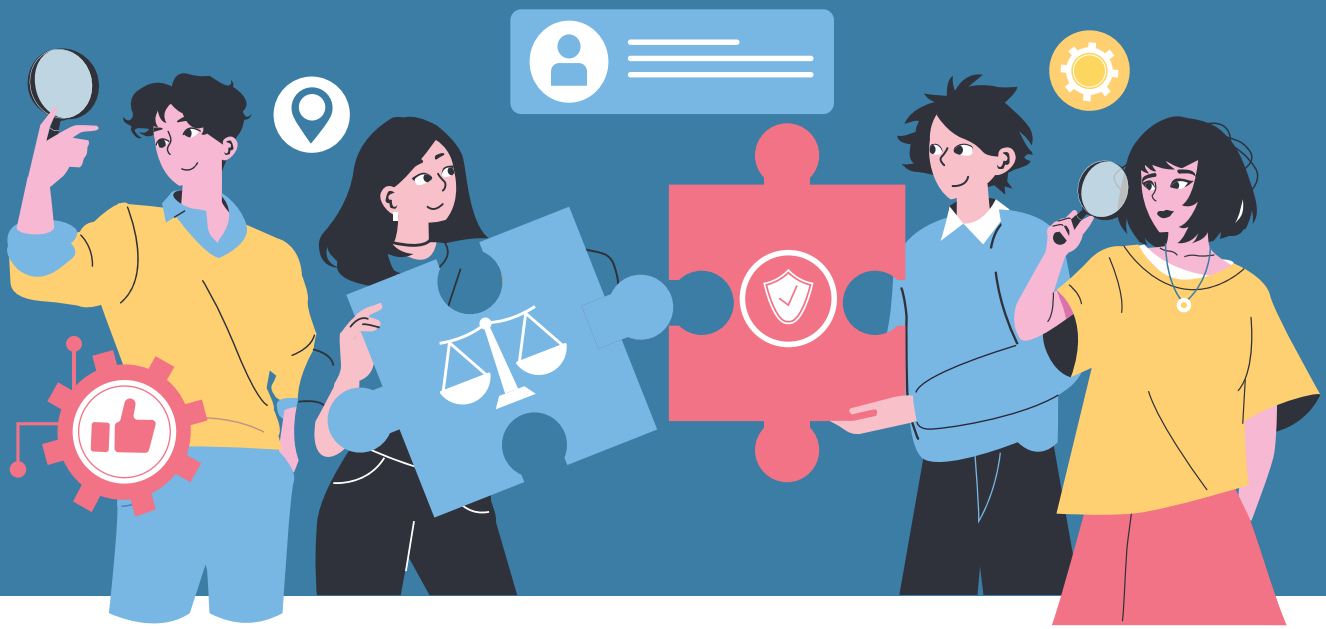
Furthermore, the AIC supported the EDPS (as an EU body) in providing replies to the EDPS (as MSA) on its inquiry on prohibited AI practices and high-risk AI tools. It also participated in inter-institutional cooperation in the field (e.g. the AI Act Correspondents Network).

***

Detailed information of activities carried out by the Data Protection Officer is provided in chapter 10 of this Annual Report.

CHAPTER TEN

DATA PROTECTION OFFICER



In 2025, the Data Protection Officer (DPO) focused on enhancing the EDPS's compliance and practical application of data protection law, while always keeping in mind the role and mission of the EDPS as the data protection authority of EU institutions, bodies, offices and agencies (EUIs).

The DPO continued to work with the EDPS's responsible services to ensure that the EDPS leads by example in upholding the highest standards of data protection.

The DPO also strengthened the EDPS's accountability by raising the standard of compliance of its personal data processing activities.

This chapter highlights how the DPO:

- monitored the EDPS's application of data protection rules;
- counselled responsible services regarding personal data processing activities under their remit;
- handled, together with responsible services, individuals' enquiries and complaints.

10.1. Accountability

As the body in charge of supervising the way EUIs handle personal data, we remain committed to upholding compliance with data protection legislation, established practice guidelines and applicable case-law.

10.1.1. Monitoring the application of data protection rules

The DPO constantly monitors the practical application of data protection rules and procedures in light of the legal provisions of Regulation (EU) 2018/1725 (the Data Protection Regulation for EUIs), case law (e.g. Court of Justice of the EU rulings) and relevant guidance (e.g. guidance issued by the EDPS as DPA and European Data Protection Board).

10.1.2. Register for processing activities

The EDPS's register of personal data processing activities was regularly updated with new and updated records on various topics related to the EDPS's supervisory activities, administration (including human resources), IT, communication and security.

10.1.3. Updating data protection notices

As controller, the EDPS aims to increase transparency and accessibility towards individuals and EDPS employees about how it processes their personal data. With this in mind, the EDPS continued to publish on its website and intranet new and updated data protection notices that are clearer and more comprehensive. These data protection notices inform readers on how their personal data is processed and for what purposes, such as for the organisation of events and webinars, or for social media.

10.1.4. Ensuring the compliance of services used by the EDPS

The DPO continued the process of scrutinising the services used by the EDPS in order to clarify the responsibilities of the service providers on data protection matters, and adapting, where appropriate, contractual clauses governing this collaboration. This is particularly relevant when the EDPS uses external service providers, such as for IT or human resources (HR) services, artificial intelligence (AI) or communication tools. Likewise, the EDPS, as controller, continued its exploration of alternative options to using large-scale providers, within the context of the EU's 'digital sovereignty'.

10.1.5. Assessing data protection risks

Together with the responsible services, the DPO assessed the risks to the fundamental rights and freedoms of individuals of new and ongoing processing activities, including analysing the need to carry out Data Protection Impact Assessments.

10.2. Advising the EDPS

The DPO continued to advise and work closely with responsible services to ensure the EDPS's compliance with the data protection framework. In particular, the DPO counselled the EDPS's responsible services on the data protection compliance of new services that the EDPS was considering using, such as in the fields of HR, IT and communication.

In this context, safeguards were put in place to ensure data protection compliance, including specific contractual terms tailored to the relevant circumstances.

The DPO was also regularly consulted on the legal provisions of new and updated agreements with EUIs that are also service providers to the EDPS, such as on IT and AI tools, as well as new and updated contracts with external service providers, and the review of certain internal rules and procedures.

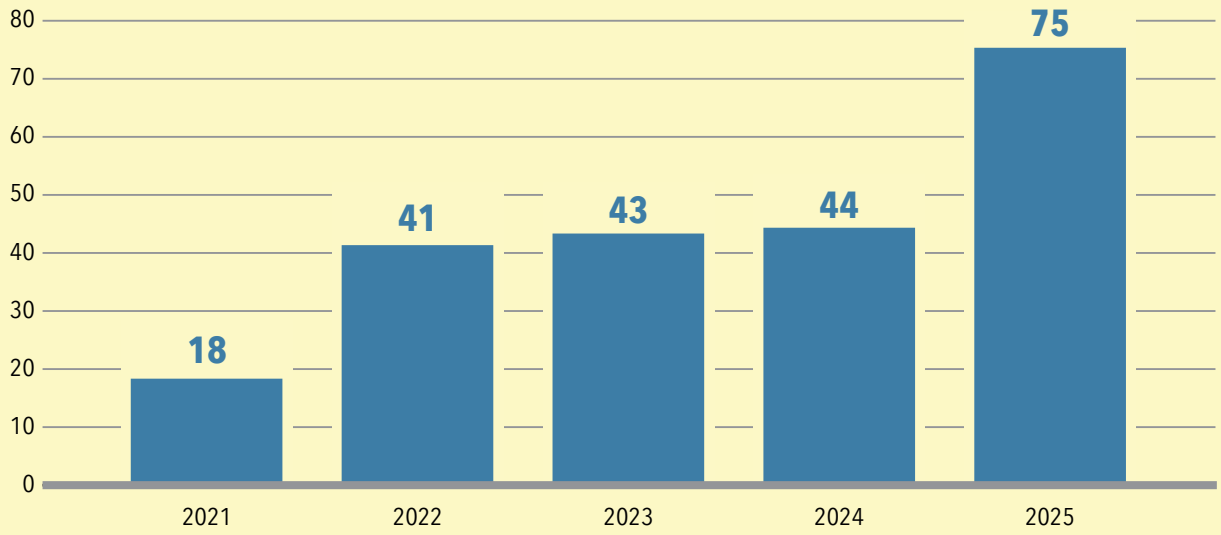
10.3. Enquires and complaints

The EDPS's DPO assists the controller to respond to enquiries and complaints made by individuals whose personal data has been or is processed by the EDPS as an EU body while fulfilling its tasks.

10.3.1. Enquiries

The overall number of enquiries and requests from individuals asserting their data protection rights received by the EDPS increased significantly in comparison to previous years.

Graph 19
Data subject requests (2021–2025)*

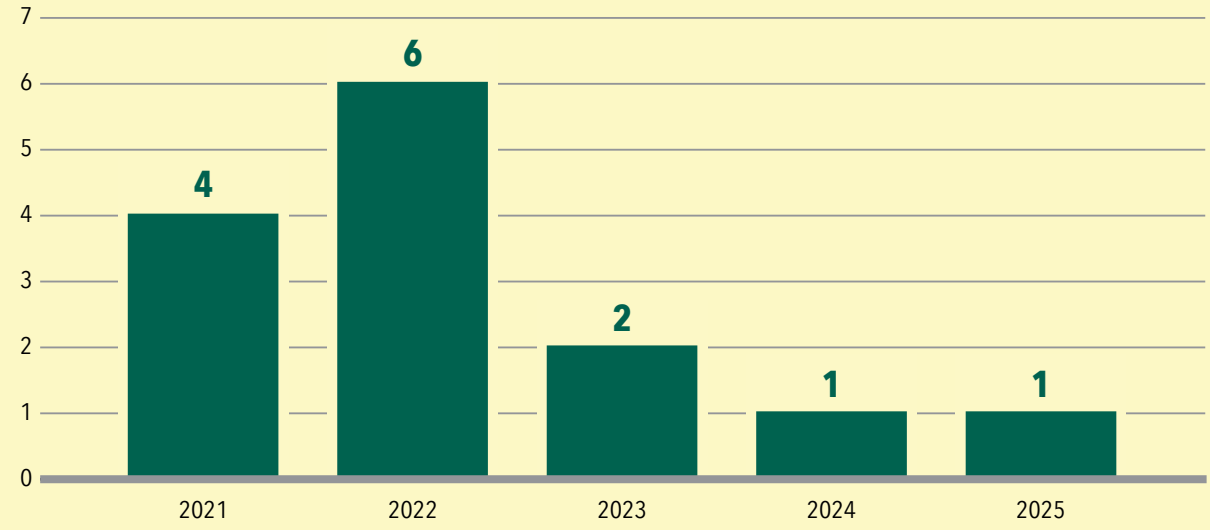


(* data excludes inadmissible requests)

10.3.2. Complaints

In 2025, the EDPS, as controller, received no complaints. However, the EDPS, as DPA, received a complaint regarding processing of personal data by the EDPS as controller in the context of a data subject request. In this context, the EDPS (as controller) provided its view on the allegations.

Graph 20
Complaints (2021–2025)



10.4. Raising awareness about data protection

In 2025, the DPO delivered a number of training sessions and carried out other activities within the institution to raise awareness about data protection. Data protection is part of the training provided to newcomers to the EDPS; this module that is updated regularly to take into account the latest developments in the field, including the most recent internal rules and procedures of the EDPS, and relevant case-law.

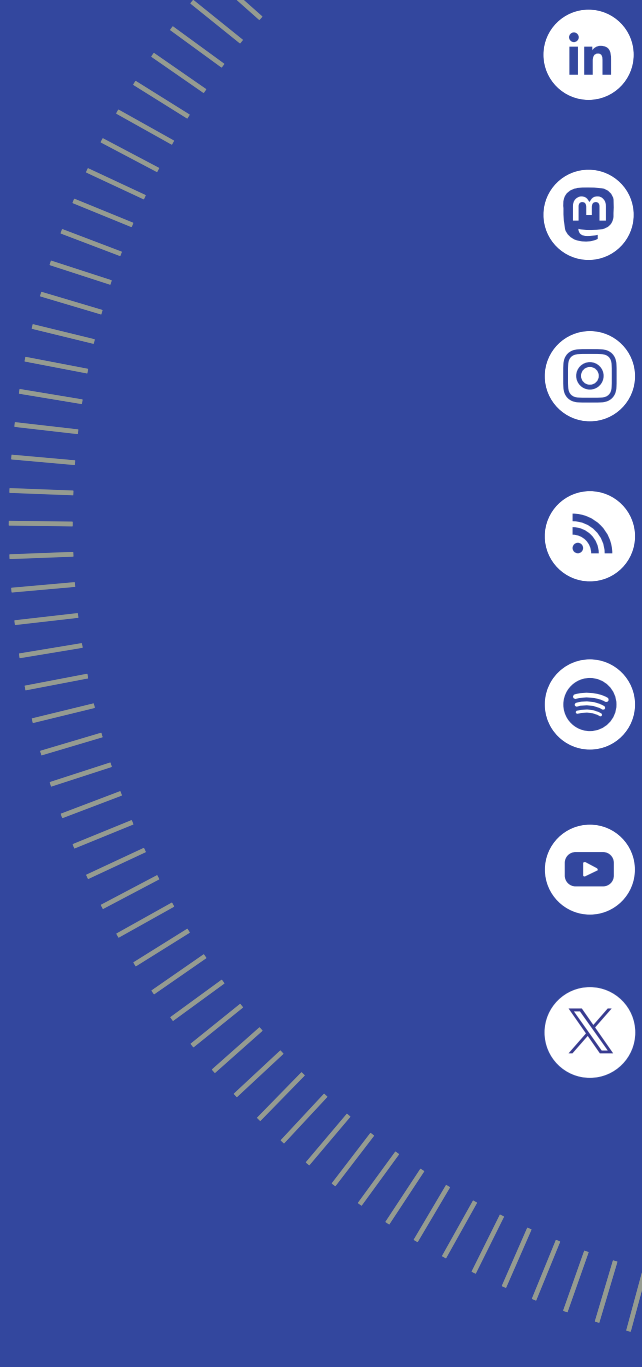
To raise awareness on data protection, the DPO also organised an 'artistic competition' for Data Protection Day 2025, giving the opportunity to EDPS staff to pair up their expertise in data protection and artistic talents. This activity, held every year, is appreciated by colleagues and a variety of fascinating entries were presented in 2025, focusing primarily on the interplay between data protection and AI. This competition also reinforces collegiality between the EDPS staff and provides an opportunity to discuss data protection in a unique manner.

10.5. Cooperation with other data protection officers and the supervisory authority

The DPO continued its collaboration with those of other EUIs, allowing for the valuable exchange of expertise and best practices in various formats, including regular meetings and working groups on specific topics, bringing together DPOs and other experts.

In July and November 2025, the DPO participated in a biannual two-day meeting cycle: an initial meeting between the EUI DPOs, followed by a second day dedicated to the EDPS-DPO Network, in which the EDPS joins as supervisory authority. The meetings focused on topical matters, such as data protection impact assessments, AI and data protection, the DPO position, and individuals' requests.

In order to foster cooperation and communication between the EDPS, as a DPA, and the EUIs' DPOs, three EDPS-DPO roundtables were also organised. These roundtables provide a forum to discuss the application of data protection rules, possible solutions to ensure that individuals' data is adequately protected according to the EU's values and principles. Various topics were discussed, such as AI and data protection, the DPO position, websites compliance, transfers outside of the European Economic Area (EEA), and individuals' requests.



Publications Office
of the European Union