



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority

"2025 Annual Activity Report"

Contents

Abbreviations	4
Introduction	6
Highlights of the year	6
Key performance indicators	7
Operational achievements	8
European Data Protection Supervisor	8
Supervisory tasks	8
Legislative advisory tasks	22
Advocacy and Cooperation.....	24
Technology monitoring tasks.....	31
Artificial Intelligence	32
Data Protection Officer Activities	36
Access to documents	37
Communication.....	37
Secretariat of the European Data Protection Board	38
Support to the EDPB activities	38
Helsinki statement	38
Binding decisions	39
Consistency opinions	39
General guidance	39
Legislative consultation	40
Enforcement cooperation.....	40
Litigation.....	42
Coordinated Supervision Committee.....	42
Data Protection Officer Activities.....	42
Access to documents	42
Communication, Information Technology & Administration.....	42
EDPS-EDPB Joint Opinions	43
Resources management	43
Human resources	43
Talent attraction, recruitment and onboarding	43
Talent Retention and HR Enhancements.....	44
Development of employees, teams and of the organisation	44
Budget	45
Budget discharge	45
Budget allocation	45
Budget implementation	45

Budget for 2026.....	46
Finance.....	46
Ex-ante controls	47
Procurement and contracting	47
Missions' management	48
IT infrastructure and tools	49
Assets' Security & Business Continuity.....	50
Internal control.....	51
Control results.....	51
Effectiveness.....	51
Efficiency.....	53
Audit observations	53
Internal Audit Service	53
European Court of Auditors.....	54
Annual planning and risk management	54
Internal control annual assessment	54
Conclusions on the assurance.....	55
Declaration of assurance.....	56
Annexes	57
Human resources at the EDPS/EDPB	57
Budget in 2025	59
List of missions undertaken by the Supervisor in 2025	62

Abbreviations

AEPD	Spanish Data Protection Authority
AI	Artificial Intelligence
AIGO	Working Party on Artificial Intelligence Governance
AMP	Annual Management Plan
AOD	Authorising Officer by Delegation
CEF	Coordinated Enforcement Framework
CERT-EU	The Computer Emergency Response Team of the EU Institutions, bodies and agencies
CJEU	Court of Justice of the European Union
CMS	Case Management System
CoE	Council of Europe
CPDP	Computers, Privacy and Data Protection
CSC	Coordinated Supervision Committee
DG	Directorate-General
DMA	Digital Market Act
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
ECA	European Court of Auditors
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity
EP	European Parliament
EPPO	European Public Prosecutors' Office
EPSO	European Personnel Selection Office
ETIAS	European Travel Information and Authorisation System
EU	European Union
EUDPR	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data
EUIBAs	European Institutions, bodies and agencies
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
Frontex	European Border and Coast Guard Agency
FTE	Full-time equivalent
GDPR	' General Data Protection Regulation ' Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
GPA	Global Privacy Assembly
HLG	High Level Group
HR	Human Resources
IAS	European Commission Internal Audit Service
ICDT	Inter-institutional Committee for Digital Transformation

ICS	Internal control standards
IDOC	Investigation and Disciplinary Office of the European Commission
IICB	Inter-institutional Cybersecurity Board
IPEN	Internet Privacy Engineering Network
IT	Information Technology
KPI	Key Performance Indicator
LCO	Local Cybersecurity Officer
LISO	Local Information Security Officer
LLMs	Large Language Models
MEPs	Members of the European Parliament
MoU	Memorandum of Understanding
OECD	Organisation for Economic Co-operation and Development
OLAF	European Anti-Fraud Office
PATRICIA	'Personal dATA bReach awareness IN Cybersecurity Incident hAndling'
PET	Privacy Enhancing Technology
PKI	Public Key Infrastructure
PMO	Paymaster Office of the European Commission
RoP	Rules of Procedure
SIS	Schengen Information System
SLA	Service Level Agreement
SMCs	Small Mid-Cap Enterprises
SMEs	Small and Medium-Sized Enterprises
SoA	Statement of Assurance
SPE	Support Pool of Experts
SR	Staff Regulation
SRB	Single Resolution Board
T-PD	Consultative Committee of the Convention 108
VIS	Visa Information System
WCAC	Website Compliance Awareness Campaign
WEC	Website Evidence Collector
WG	Working Group
WPDGP	Working Party on Data Governance and Privacy

Introduction

The present report is drawn up pursuant to Article 74(9)¹ of the Financial Regulation which stipulates that each authorising officer by delegation (AOD) shall submit an annual activity report to their Union institution, together with financial and management information. This report presents the achievements of the institution in relation to the resources used. It also constitutes a management report on performance in the context of the tasks of AOD. This is in line with Article 74(2) of the Financial Regulation, which gives the AOD responsibility for internal controls.

A Statement of Assurance (SoA) is included in the present report, confirming that the AOD has reasonable assurance that:

- the information contained in the report presents a true and fair view;
- the resources allocated to the activities described in the report have been used for their intended purposes and in accordance with principles of sound financial management, and that the control procedures put in place give the necessary guarantees as to the legality and regularity of the underlying transactions;
- there are no matters that are not reported, and which could harm the interests of the institution.

Highlights of the year

2025 was a transitional period for the EDPS since the selection procedure for a new Supervisor was not finalised. Despite this, the EDPS made steady progress in data protection, transparency, and enforcement, continuing its central role in EU digital governance.

The EDPS' strong commitment to promoting responsible data governance was internationally recognised by the Global Privacy Assembly (GPA) through **the GPA Global Privacy and Data Protection Awards 2025**, where the EDPS received an award in the Accountability category. This recognition also stems from two strategic initiatives launched by the EDPS to enhance personal data breach management across EU institutions, bodies, and agencies (EUIBAs).

Following its designation as the supervisory authority for the EUIBAs under the AI Act, the EDPS organised and hosted in Brussels the first **two meetings** of the **AI Act Correspondents Network**, a dedicated forum to facilitate communication and coordination between the EUIBAs and the EDPS. These meetings brought together representatives from all EUIBAs to discuss practical implementation of the AI Act, compliance challenges, and how to balance innovation with fundamental rights.

Another key development was the EDPS' proposal to establish a **Digital Clearinghouse 2.0**, a coordination platform for authorities enforcing EU digital laws, building on the successful precedent of the first Digital Clearinghouse from 2017. Such a platform would provide authorities and bodies with a forum to exchange and coordinate on issues of common interest, help align policies, share legal interpretations, and improve enforcement cooperation between regulatory bodies.

To increase transparency, the EDPS introduced a new **Transparency Decision**, requiring that scheduled bilateral meetings between EDPS senior staff and interest representatives can be held only if the latter are registered in the Transparency Registry, with the details of these meetings publicly disclosed on the EDPS official website. This development supports greater accountability and openness in the institution's work.

A major achievement was the **closure** of the enforcement case on the **European Commission (EC)'s use of Microsoft 365**. Following the EDPS investigation, the EC adjusted its use of the software to comply with EU data protection rules. Additionally, the EC revised contractual arrangements that are available to other EUIBAs, raising data protection standards across the board. Overall, the EDPS continued to exercise its

¹ Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast): <https://eur-lex.europa.eu/eli/req/2024/2509/oj/eng>

investigative and enforcement powers, demonstrating its continued efforts to ensure compliance with data protection regulations while facing an increasing number of complaints.

Despite being a year of transition, the EDPS made significant progress - from leading on AI governance, improving transparency, and delivering strong enforcement results. The work done in this period strengthens data protection in EU institutions and sets a solid foundation for future challenges. The EDPS remains focused on ensuring compliance, transparency, and fundamental rights in the digital age.

Key performance indicators

The EDPS uses nine key performance indicators (KPIs) for monitoring performance as set by the EDPS Strategy 2020-2024². The KPI scoreboard below 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.

In 2025, the organisation **met or surpassed the targets set in all KPIs, except one**, confirming the positive trend in implementing strategic objectives throughout the year.

KPI 7, on EDPS social media’ followers, did not fully meet the set target, as the 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, the EDPS reactivated the **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 **6 211 followers** already gathered under the former EU Voice account.

KEY PERFORMANCE INDICATORS		Results 31.12.2025	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 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, Spring Conference, international organisations) for which EDPS has provided a substantial written	34 cases	10 cases

² KPIs are regularly revised to ensure that performance metrics adapt to developments in EDPS activities. In the transition period due to the ongoing selection procedure for the Supervisor, the EDPS kept as main framework the Strategy set for the 2020-2024 mandate.

	contribution		
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 EC 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	LI: 90 838 X: 28 102 YT: 3 681 Instagram: 731 Total: 123 352 <i>Mastodon: 6 211</i>	Results of previous year ³ + 10% 2025 target: 127 010
KPI 8 Internal Indicator	Occupancy rate of establishment plan	92.50%	90%
KPI 9 Internal Indicator	Budget implementation	92,50%	90%

³ Results of the previous year (2024): 115 464 followers [LinkedIn: 82 881, X (ex-twitter): 28 860, YouTube: 3 409, Instagram: 314].

Operational achievements

European Data Protection Supervisor

Supervisory tasks

In 2025, the EDPS continued to supervise EUIBAs on their compliance with the EU's data protection legal framework, particularly Regulation (EU) 2018/1725⁴ (the 'EUDPR'). As outlined in the Strategy⁵, the EDPS remains committed to supporting EUIBAs in setting an example for safeguarding digital rights and promoting responsible data processing practices. The following section describes several key supervisory and enforcement actions undertaken by the EDPS in 2025.

1. Complaints

Handling complaints from individuals is a central element of the EDPS supervisory mandate. Complaints allow individuals to challenge how EUIBAs 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 complaints have continued to increase, reflecting greater awareness of data protection rights and more complex processing environments within EU administration.

In 2025, the EDPS 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 respond efficiently to a complaint depends on several factors⁶, including the complexity of the processing at issue. Despite these challenges, the EDPS exceeded expectations in 2025 by concluding enforcement activities, issuing decisions and closing follow-up in 79 admissible complaint cases⁷.

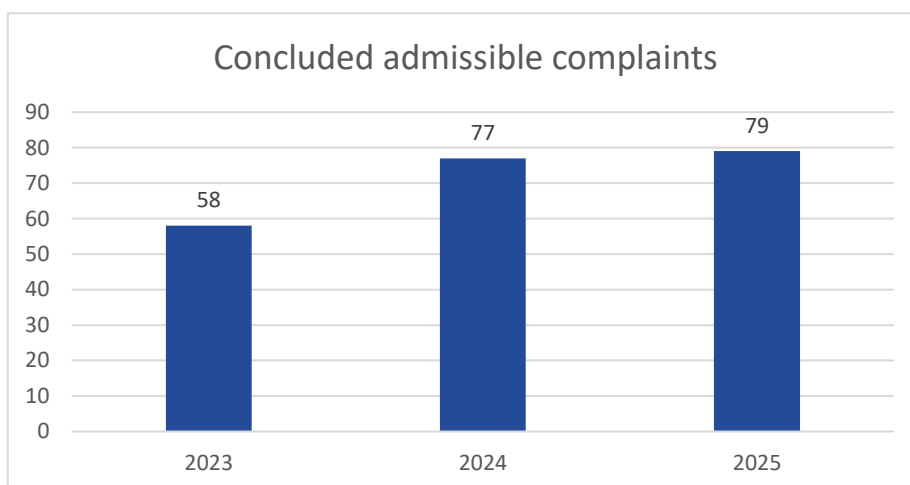
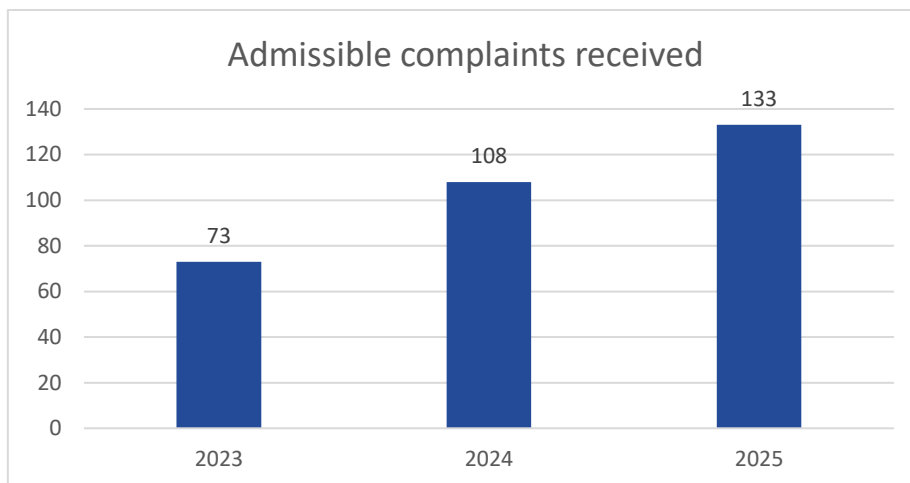
⁴ [Regulation \(EU\) 2018/1725](#) of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

⁵ https://www.edps.europa.eu/press-publications/publications/strategy_en

⁶ These factors are:

- the complexity of the subject matter;
- the need to obtain the views of the parties to the case and, where relevant, of any other entity involved entails multiple exchanges where the responsiveness of the controller/complainant/other entity goes beyond EDPS 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 required for the EDPS to understand the matter and assess whether the EUI infringed any applicable rules;
- the need for any on-the-spot checks or remote investigations of the complaint;
- any concurrent or planned EDPS enforcement actions on the same or similar matter;
- the need for any suspension of handling and investigating a complaint because of a pending case before courts or administrative bodies; - as well as on the resource constraints of the EDPS.

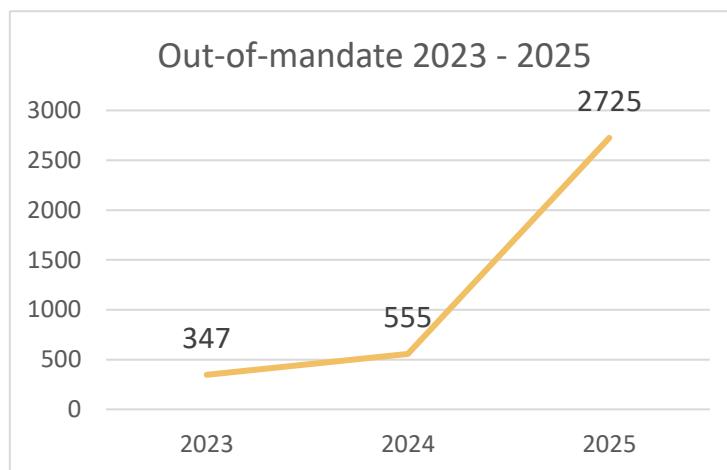
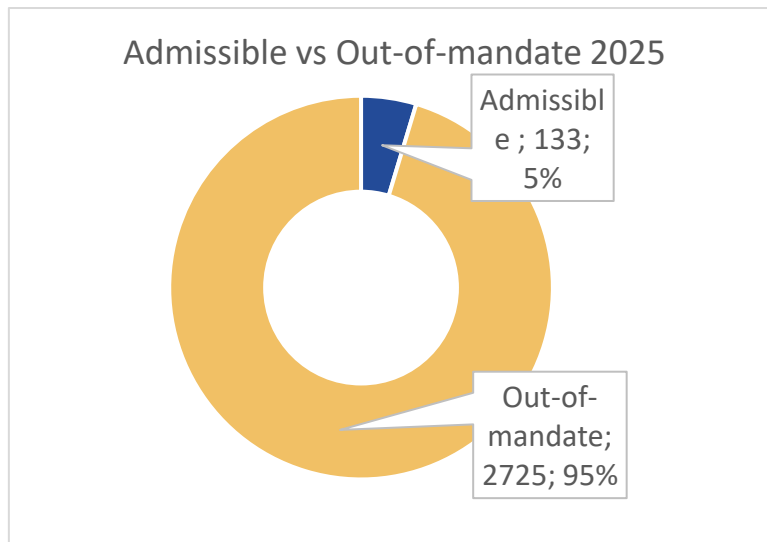
⁷ A complaint procedure can be concluded either by referral to the data protection officer of the EUIBA; by referral to a controller in the EUIBA; by amicable settlement or other resolution during the investigation phase; by formal decision of the EDPS or by pursuit of the matter through other EDPS enforcement actions (such as an audit or own-initiative investigation). After issuing a decision in a complaint case, the EDPS systematically checks how the EUIBAs concerned implement corrective measures imposed by the EDPS in its decision.



In addition to admissible complaints, the organisation received **2 725 inadmissible** complaints in 2025, compared to 555 in 2024. This constitutes a **significant rise** of complaints falling outside the EDPS mandate⁸. This sharp increase appears to be linked, in part, to the growing use of automated and AI-based tools that may misdirect individuals to submit complaints to the EDPS regardless of jurisdiction. While the EDPS cannot take enforcement action on out-of-mandate complaints, all such complaints must still be analysed and responded to within the prescribed timeframe. In 2025, the EDPS further streamlined its response procedures and strengthened public information on the scope of its mandate to better guide individuals to the competent authority when the EDPS is not empowered to act, including an eligibility questionnaire⁹.

⁸ Complaints relating to matters outside the EDPS' competence are considered inadmissible from the outset. Out-of-mandate complaints typically concern processing carried out by private entities, national authorities or international organisations, ie they fall outside the EDPS competence.

⁹ How to submit a complaint https://www.edps.europa.eu/data-protection/our-role-supervisor/complaints_en



Admissible complaints mainly concerned individuals’ rights, especially the right of access to personal data and the right to be informed about processing activities, followed by issues relating to the security and confidentiality of processing. As in previous years, most admissible complaints were submitted by EUIBAs’ staff and concerned the EC, reflecting its size and range of activities¹⁰.

The following key decisions illustrate how complaints handling contributes to clarifying key data protection principles in practice:

In March 2025, EDPS issued a **decision concerning the transmission of EU staff members’ personal data to the Permanent Representations of Member States**. The case concerned the regular transmission by an EUIBA of several categories of staff data, including contact details, employment information and nationality. The EDPS found that, under the [EU rules establishing privileges and immunities](#)¹¹ only a limited set of data – names, grades and addresses – may be transmitted. As the EUIBA could not demonstrate a valid legal basis for transmitting additional categories of personal data, the EDPS concluded that the processing infringed the principles of lawfulness, data minimisation and purpose limitation. The EDPS issued a reprimand and ordered the EUIBA to cease transmitting data beyond what is strictly required. Given the wider relevance of the issue, the EDPS also issued guidance to all EUIBAs on assessing and limiting such transmissions.

¹⁰ This is partly explained by the EC’s role as the largest EU institution and as a provider of centralised services to other EUIs, such as staff recruitment, the administration of allowances and remuneration, and the management of the joint health insurance scheme for EU staff.

¹¹ Based on [Article 15\(2\) of Protocol No 7 to the TFEU](#).

Another decision issued in April 2025 concerned data protection **by design and by default**¹² in the context of the **EC's EU Funding & Tenders Portal**. Following a complaint against the Commission's Directorate-General for Informatics, the EDPS assessed the procedure for activating a Legal Entity Appointed Representative (LEAR) account. It was 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. In addition, internal instructions were found to be clear, regularly reviewed and adequate to ensure the security of the processing.

In June 2025, the EDPS examined a **complaint** against the **European Personnel Selection Office (EPSO)** regarding access to a selection board's **handwritten notes**. Balancing the complainant's right of access with EPSO's need to preserve confidentiality and impartiality of selection procedures, the EDPS concluded that a joint typed summary of the notes would allow access while preserving the secrecy of the proceedings.

In December 2025, another milestone decision addressed the unlawful disclosure of email addresses following a public access to documents request. The disclosure was deemed unnecessary and breached key data protection principles. Although the EUIBA concerned implemented corrective technical and organisational measures, a reprimand was issued to underline the importance of carefully assessing the necessity of disclosing personal data¹³.

2. Court cases

Court proceedings in 2025 played a significant role in clarifying key data protection concepts and reinforcing supervisory principles. Through strategic litigation and defence of the EDPS decisions, the institution contributes to legal certainty for EUIBAs and to the consistent protection of individuals' rights across the EU legal order. The following cases provide an illustration of the year's highlights.

A landmark judgment was delivered on 4 September 2025 by the Court of Justice of the European Union (CJEU) in the case **EDPS v Single Resolution Board (SRB)** (C-413/23 P). The Court set aside¹⁴ the General Court's 2023 judgment¹⁵. The case concerned the transfer by the 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, and that the obligation to inform data subjects applies at the moment personal data are collected. The judgment reaffirmed the EDPS interpretation of the right to information and has broader implications for supervisory practice.

In 2025, proceedings continued in the appeal case **EDPS v Parliament and Council** (C-698/23 P). The appeal concerns EDPS' standing to challenge two provisions of the amended Europol Regulation, which according to the EDPS affect Europol's personal data operations, undermine legal certainty for individuals' personal data and interfere with the EDPS' independence. In May 2025, the Advocate General issued an opinion¹⁶, confirming that EDPS has *locus standi*, as the contested provisions directly and individually concern the organisation. The judgment is expected to clarify the EDPS' role as the EU data protection supervisory authority and the conditions under which it may take action.

Another significant development occurred on 28 July 2025, when **the EC and Microsoft Ireland Operations discontinued their actions against the EDPS decision of 8 March 2024** concerning the Commission's use of **Microsoft 365**. As a result, in September 2025, the General Court removed¹⁷ the joined cases T-262/24 and

¹² See also [EDPS Preliminary Opinion on Privacy by Design](#) and [EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#).

¹³ See [EDPS, Public access to documents containing personal data after the Bavarian Lager ruling](#).

¹⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62023CJ0413>

¹⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62020TJ0557>

¹⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CC0698>

¹⁷ https://infocuria.curia.europa.eu/tabs/document/T/2024/T-0262-24-00000000RD-01-P-01/ORD_NP/304797-EN-1-html

T-265/24 from its register. These developments reaffirmed the relevance of the EDPS supervisory findings while bringing procedural closure to the litigation.

3. Investigations

Investigations are the EDPS primary tool for supervision and enforcement, enabling the assessment of how EUIBAs apply EU data protection rules in practice, particularly in cases of serious concerns¹⁸. Investigations bring together legal and technical expertise and follow a structured process, including evidence gathering, inspections and preliminary assessments¹⁹. Unlike complaint handling²⁰, own-initiative investigations are launched independently and may be preceded by pre-investigation²¹ work. Through investigative activities, the EDPS aims not only to address specific compliance issues, but also to strengthen transparency, accountability and trust in the way EUIBAs process personal data.

These often complex and resource-intensive activities require close cooperation with national authorities, and increasingly address large-scale processing operations. Despite growing demands, the EDPS maintained strong performance in 2025, advancing and concluding multiple cases while ensuring systematic follow-up. Beyond individual outcomes, investigations drive structural improvements, promote a culture of compliance, and strengthen the protection of fundamental rights across EU administration.

Key investigation outcomes

By addressing concrete risks, clarifying governance obligations and encouraging corrective action, the EDPS investigative work strengthens data protection practices across EUIBAs and supports a consistent and rights-respecting approach to the processing of personal data. Below, are listed some milestone cases:

First, on 3 February 2025, the EDPS **closed a pre-investigation into the European Personnel Selection Office' (EPSO) use of remotely proctored testing**. This decision considered the results of a previous EDPS audit and complaint decision, as well as the measures implemented by EPSO in response. The case was closed in light of the progress made in addressing the identified issues, without prejudice to EDPS' ability to take further supervisory action if necessary.

Second, on 6 February 2025, the EDPS **closed investigations into international transfers linked to EUIBAs' 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, the EDPS observed increased awareness among EUIBAs of their obligations regarding transfers outside the European Economic Area (EEA), 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, depending on relevant developments.

Third, in July 2025, the EDPS **closed** enforcement proceedings following the investigation into the **EC's use of Microsoft 365**. After examining the Commission's implementation of additional contractual, technical and organisational measures, it concluded²² that the infringements identified in the 2024 decision²³ had been

¹⁸ 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 EUIBAs.

¹⁹ 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 EC.

²⁰ For further details on the EDPS's handling of complaints, please refer to the dedicated section on [complaints](#)

²¹ Before launching a formal investigation, a pre-investigation may be conducted to gather facts and to evaluate compliance and the credibility of allegations.

²² https://www.edps.europa.eu/data-protection/our-work/publications/investigations/2025-07-11-closure-enforcement-proceedings-commissions-use-microsoft-365_en

²³ https://www.edps.europa.eu/data-protection/our-work/publications/investigations/2024-03-08-edps-investigation-european-commissions-use-microsoft-365_en

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 EUIBAs, and those using Microsoft 365 are encouraged to carry out comparable assessments and to implement similar measures. Targeted advice was also provided to EUIBAs in September and December 2025 to support a common and secure baseline for the use of these services.

Fourth, investigations were concluded into **the dismissal of Data Protection Officers (DPOs)** at the Committee of the Regions²⁴ and the European Defence Agency²⁵. Breaches were found in both cases for failing to obtain the EDPS's prior consent before dismissing a DPO. The decisions reaffirm that DPO independence is a cornerstone of effective data protection governance within the European administration. Reprimands were issued, though mitigating factors - such as acknowledgment of responsibility and corrective action by the EUIBAs - were also considered.

Finally, on 25 July 2025, EDPS closed a pre-investigation into the selection of Blue Book trainees. The 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 the EDPS subsequently decided to launch an audit at the EC's Traineeship Office.

4. Cooperation with data protection authorities

Supervisory cooperation with national Data Protection Authorities (DPAs) is an essential element of effective and consistent enforcement of EU data protection law. In 2025, the EDPS cooperated with DPAs within and outside the European Union/European Economic Area (EU/EEA), both in concrete cases and through structured cooperation frameworks, in particular within the European Data Protection Board (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.

a. Cross-Border

In 2025, the EDPS cooperated with national DPAs on complex cross-border processing operations, including the use of cloud services by public bodies and proceedings concerning the EC's use of Microsoft 365. Assistance was also provided to two DPAs in the EEA, regarding data processing by EUIBAs. Cooperation will continue in 2026, alongside further supervisory assessment. The EDPS also contributed to cases in the area of freedom, security and justice to support coherent EU and national oversight.

b. Within the EDPB

In 2025, the EDPS contributed to the work of the EDPB, drawing on supervisory and enforcement experience to support EDPB guidance and discussions on issues such as anonymisation and pseudonymisation, data disclosures, safeguards for international transfers, and controller–processor and joint controllership arrangements. This cooperation helps ensure consistent supervision of similar technologies and processing operations across the EU/EEA.

c. Coordinated Enforcement Actions

In 2025, the EDPS participated in a Coordinated Enforcement Action²⁶ (CEF) under the EDPB framework. These actions aim to promote consistent enforcement of data protection rules across the EEA by focusing on selected topics of common relevance.

²⁴ https://www.edps.europa.eu/system/files/2025-09/25-07-24_investigation-dismissal-of-cor-dpo_en.pdf

²⁵ https://www.edps.europa.eu/data-protection/our-work/publications/investigations/2025-11-24-552025-european-data-protection-supervisor-edps-investigation-case-2025-0787-against-european-defence-agency-eda_en

²⁶ https://www.edps.europa.eu/press-publications/press-news/press-releases/2025/edps-participates-fourth-coordinated-enforcement-action-focus-right-erasure-personal-data_en

The EDPS participated in the 4th CEF, which focused on the **right to erasure**²⁷. Through a survey-based fact-finding exercise it was examined how EUIBAs handle erasure requests, including volumes, refusals and applicable procedures. Results indicated that EUIBAs generally receive few requests, with many refusals linked to public interest tasks or legal obligations. While standard procedures are often in place, challenges remain in applying exceptions, managing combined access and erasure requests, and demonstrating accountability, particularly regarding secure erasure techniques. The findings were shared with EUIBAs and their DPOs and will inform future supervisory and enforcement actions.

In 2025, the CEF on the implementation of the right of access²⁸ was concluded with the issuance of the EDPB report, which reflected the EDPS findings from the fact-finding exercise carried out the previous year.

Finally, in October 2025, the EDPB selected transparency and information obligations as the topic for the 2026²⁹ CEF. The EDPS contributed to the preparatory work for this coordinated action. A decision on the EDPS' formal participation will be taken in the course of 2026, taking into account priorities and available resources.

5. Supervisory opinions and guidance

a. Supervisory opinions

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

In 2025, the EDPS supervisory opinions addressed key governance and transparency challenges arising in the context of the European Central Bank's supervisory and investigative activities. Below, key opinions are presented:

i. Joint control in banking supervision

The opinion 18/2025³⁰ was issued following a consultation by the **European Central Bank** (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 are 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, it was clarified that joint controllership **does not remove individual responsibility**. 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 EUIBAs are met. This obligation applies independently of any notification duties that NCAs may have under the General Data Protection Regulation (GDPR).

²⁷ https://www.edps.europa.eu/press-publications/press-news/press-releases/2025/edps-participates-fourth-coordinated-enforcement-action-focus-right-erasure-personal-data_en

²⁸ https://www.edps.europa.eu/press-publications/press-news/press-releases/2025/coordinated-enforcement-action-edps-findings-highlight-challenges-right-access-personal-data_en

²⁹ https://www.edpb.europa.eu/news/news/2025/coordinated-enforcement-framework-edpb-selects-topic-2026_en

³⁰ https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2025-11-10-opinion-182025-joint-controllership-arrangement-between-european-central-bank-and-national-competent-authorities-context-single-mechanism_en

Second, the EDPS 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, it was recommended that these responsibilities be **clearly** and explicitly reflected in the joint controllership arrangement itself.

This opinion underlines that joint controllership is a tool for cooperation, and that each controller remains accountable under the legal framework that applies to it. By clearly allocating tasks EUIBAs 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.

ii. Transparency in ECB investigations

The opinion 6/2025³¹ highlights the need to strike a careful **balance between protecting** the effectiveness of internal investigations and **safeguarding 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, EUIBAs 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 European administration.

The opinion was issued following a consultation by the ECB on proposed amendments to its internal framework for **reporting, investigation, and disciplinary follow-up** in data protection matters. The consultation raised questions about how and when individuals should be informed when their personal data are processed in the context of internal investigations, particularly where data have not been obtained directly from the data subject. The EDPS clarified that **confidentiality** during investigations must remain **an exception** and any decision to withhold information be clearly justified and documented.

b. Safeguards for international transfers

i. Administrative Arrangement model for transfer to public authorities in third countries

In 2025, the EDPS introduced the 'Model'³² Administrative Arrangement for transfers of personal data from EUIBAs to public authorities in third countries'. The Model, adapted to the legal context of third-country public authorities and to national obligation, is designed to help controllers put in place data protection appropriate safeguards. It sets out **minimum requirements** to protect personal data and reflects the approach developed at EU level for transfers between public authorities. . While arrangements based on the Model still require the EDPS approval, its use simplifies the process and benefits all parties.

ii. EDPS decisions authorising transfers to third countries

³¹ https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2025-04-16-opinion-62025-proposed-amendments-european-central-banks-legals-framework-reporting-investigation-and-disciplinary-follow-data-protection_en

³² https://www.edps.europa.eu/data-protection/our-work/publications/international-transfers/2025-12-16-edps-model-administrative-arrangement-transfers-personal-data-euis-public-authorities-third-countries_en

Through decisions 65/2025³³, 66/2025³⁴ and 67/2025³⁵ the **EDPS authorised transfers of personal data** from the EC to Türkiye, North Macedonia and Serbia for the implementation of the Erasmus+ and European Solidarity Corps programmes. These cases involved remote access to EC’s IT systems by processors in third countries and complex contractual chains with multiple sub-processors. The EDPS confirmed that in this context, well-designed contractual clauses can provide appropriate safeguards. The organisation’s work on international transfers in 2025 demonstrates the importance of combining practical tools with rigorous case-by-case assessments.

c. European Travel Information and Authorisation System watchlist opinion

The European Travel Information and Authorisation System (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.

The opinion 2/2025³⁶ assessed Europol’s draft Management Board Decision setting out the **procedures governing its responsibilities in entering data into the watchlist**. As a conclusion, several recommendations were issued aimed at ensuring compliance with data protection rules. Particular emphasis was given to 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.

d. Supervisory guidance

In 2025, the EDPS adopted new supervisory guidance to support EUIBAs 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 EUIBAs, and aims to translate legal requirements into concrete, operational recommendations. The following two guidance documents were particularly significant in 2025:

i. On the use of generative artificial intelligence

The **revised** supervisory guidance³⁷ on the use of generative artificial intelligence (AI) and the processing of personal data by EUIBAs was published in October 2025. The revision reflects rapid technological developments and practical experience gained since the first guidance was issued. It provides **clearer** and **actionable** direction to help EUIBAs design, deploy and use generative AI tools responsibly.

³³ https://www.edps.europa.eu/data-protection/our-work/publications/international-transfers/2025-12-18-edps-authorising-use-contractual-clauses-between-european-commission-and-turkish-national-agency-implementation-erasmus-and_en

³⁴ https://www.edps.europa.eu/data-protection/our-work/publications/international-transfers/2025-12-18-edps-authorising-use-contractual-clauses-between-european-commission-and-north-macedonian-national-agency-implementation_en

³⁵ https://www.edps.europa.eu/data-protection/our-work/publications/international-transfers/2025-12-18-edps-authorising-use-contractual-clauses-between-european-commission-and-serbian-national-agency-implementation-erasmus-and_en

³⁶ https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2025-03-04-edps-opinion-22025-management-board-specifying-europol-procedures-relation-etias-watchlist-case-2024-0897_en

³⁷ https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-10-28-guidance-generative-ai-strengthening-data-protection-rapidly-changing-digital-era_en

It also introduces a precise definition of generative AI to ensure interpretation **consistency**. It includes a **checklist** for assessing the compliance and lawfulness of processing activities. The guidance clarifies **roles** and **responsibilities**, (joint) controllership, and processors in AI-related scenarios. Finally, it provides advice on lawful bases, purpose limitation and handling of data subjects' rights in the context of generative AI systems.

ii. On the role of EUIBAs' Data Protection Officers

The new supervisory guidance³⁸ on the role of Data Protection Officers (DPOs) in EUIBAs builds on the 2018 position paper and experience gained since the entry into force of the EUDPR, including insights from supervisory activities and contributions from the EDPS–DPO network.

It clarifies key aspects of the DPO function, including **direct reporting to the highest management level**, the identification and management of conflicts of interest, and alignment of the DPO's term with the contract, where relevant. It also recalls the **conditions for dismissal** (see also [here](#)), reinforcing the importance of functional independence.

The guidance reflects the EDPS' commitment to providing **clear, practical** and **up-to-date** supervisory tools, supporting EUIBAs in strengthening accountability across the EU administration.

iii. ETIAS Fundamental Rights Guidance Board

In 2025, the EDPS continued to monitor the development of ETIAS through participation in the ETIAS Fundamental Rights Guidance Board, which provides independent guidance on the fundamental rights implications of ETIAS data processing. Five formal meetings took place, alongside expert working groups involving national authorities and EU agencies. In March 2025, the Board issued guidance on informing ETIAS applicants, focusing on the **right to an effective remedy** and a **fair trial**. It also provided input on the analytical framework for **screening rules** and the **design** of risk-screening operations underpinning ETIAS profiling. Throughout the year, the Board monitored the integration of data protection by design, including aspects related to the Data Protection Impact Assessment, controllership arrangements and the processing of law enforcement data.

iv. Guidance on the progressive start of the Entry Exit System

The Entry/Exit System 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 and operations began on 12 October 2025.

On 30 June 2025, the EDPS issued comments jointly with the [European Data Protection Board's Coordinated Supervision Committee](#) on the EC's information campaign materials relating to the progressive start of the system. It was 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. Broader shortcomings were also identified, including insufficient information on data **access** by authorities, the objectives of the system and the **practical exercise of rights**. These comments were made in light of the Commission's failure to consult supervisory authorities as required by the Entry/Exit System Regulation.

³⁸ https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-12-18-edps-guidance-role-data-protection-officers-eu-institutions-bodies-offices-and-agencies_en

In September 2025, a response was also provided to a consultation on draft practical guidance developed by the Commission for national authorities during the progressive rollout. The **recommendations** focused on mitigating risks arising from potentially incomplete or inaccurate data during this period. In particular, 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 were addressed.

6. Europol

In 2025, the EDPS 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. The EDPS 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 AI 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, the supervisory activities combined ex-ante oversight, inspections and follow-up, cooperation with national data protection authorities, and engagement with democratic oversight bodies.

Eight supervisory opinions were issued in 2025, 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.

Europol processes very large and complex datasets originating from multiple sources, including seized digital devices. To support operational analysis, Europol consulted the EDPS 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. Both the lawfulness of developing these models and their subsequent use were assessed. The EDPS 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 have not yet been fully categorised. The proportionality and necessity of these processing operations were also examined.

Another Europol consultation concerned 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.

The EDPS also 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. The EDPS also provided advice on procedures for entering information alerts in the Schengen Information System (SIS) based on data received from third countries, with a focus on avoiding inconsistent or disproportionate use and clarifying responsibilities between systems. In addition, Europol's proposed use of fingerprints to query the Visa Information System (VIS) was examined and safeguards to mitigate the risks associated with unnecessary biometric searches were identified.

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

Finally, **recommendations** were issued on new analytical tools and environments, including systems used to analyse material related to **child sexual abuse** and a proposed Internet-facing operational environment. The

EDPS advice focused on limiting data intake, restricting retention periods, and ensuring adequate oversight mechanisms.

Building on clarifications provided in earlier opinions, the EDPS continued in 2025 to advise Europol on issues arising from joint operational analysis with Member States. To this end, it was reiterated that such processing qualifies as joint controllership and requires a detailed Joint Controllership Arrangement setting out responsibilities towards data subjects and supervisory authorities. Such 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.

7. European Criminal Records Information System - Third Country Nationals

In 2025, the EDPS issued a **supervisory opinion** on several legal issues relating to the European Union Agency for Criminal Justice Cooperation (Eurojust) tasks under the Regulation on the European Criminal Records Information System for Third-Country Nationals. This centralised system enables Member State authorities to determine efficiently which Member State or States hold criminal record information on a third-country national.

The EDPS opinion focused on ensuring **consistency** between this **newly** introduced **task** and the **existing provisions** of the **Eurojust Regulation**. It 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 a processor for this processing operation, and the Member States as the controllers. The **technical means** used for processing the operational personal data received in this context were also **assessed** and provided guidance to ensure that appropriate safeguards are applied.

8. Data protection audits

Data protection audits are a core supervisory tool³⁹ that allow us to assess how EUIBAs apply data protection rules in practice. Taken together, the audit work described below shows how audit outputs contribute not only to individual compliance outcomes, but also to improvements in data protection practices, accountability and trust across the EU administration.

i. Audits and their impact

Audits provide an in-depth **understanding** of specific processing operations and allow to verify whether personal data are processed lawfully, securely, and in line with applicable requirements, including the principles of accountability and data protection by design obligations. They apply across all EUIBAs and support fairness, legal certainty and consistency in supervision. By examining processing operations in detail, audits enable recommendations tailored to the specific context for each EUIBA.

Audits⁴⁰ also play a **preventive role** by identifying weaknesses at an early stage, before risks to individuals' rights and freedoms materialise. Finally, audits provide independent **assurance** on whether key processing operations meet legal requirements, supporting **accountability**, informed decision-making, and **trust** in how personal data is handled.

³⁹ https://www.edps.europa.eu/press-publications/press-news/blog/5-good-reasons-edps-audit_en

⁴⁰ https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/audits_en

ii. Key audit outcomes

During 2025, the EDPS 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.

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, the EDPS issued an audit report on the **Medical Service** of the **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 EP's Medical Service and of the HUMAINT research project at the EC's Joint Research Centre, including shortcomings in retention practices, the lawfulness of processing sensitive data, and security safeguards. The EDPS recommendations aimed to establish **clearer rules, improve documentation, and reinforce protective measures**, particularly where vulnerable individuals or **sensitive data** are concerned.

A second set of audits addressed large-scale and innovative processing operations. In January 2025, the EDPS issued an audit report on the **European Centre for Disease Prevention and Control (ECDC)**, focusing on the use of data from the GISAID platform, social media monitoring for epidemic intelligence, restrictions of data subject rights, and access controls for surveillance systems. In November 2025, the EDPS also issued an audit report on the **EC's EU Login mobile application**, following up on the EDPS guidance on mobile applications. In both cases, the recommendations aimed to strengthen transparency, retention practices, information security, record-keeping, and the clear allocation of data protection responsibilities.

Finally, in September 2025, the **follow-up** on audits of **twenty-one** EUIBA' websites were completed. This work focused on checking 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, the emphasis was put on the responsibility of EUIBAs to fully implement and document all outstanding recommendations in line with the accountability principle.

The EDPS also carried out on-the-spot checks at the EC's Traineeship Office, the European Labour Authority's EURES system, and the Customs Information System, and continued follow-up on earlier audits.

iii. Audits and inspections

In July 2025, an inspection was carried out at Europol in cooperation with experts from national data protection authorities. The inspection focused on Europol's **use of the SIS, facial recognition solutions, transfers to third countries** and international organisations, and **exchanges** of data with private parties. Risks, recent developments and previous supervisory findings defined the scope.

Considering Europol's high implementation rate of previous recommendations and the extensive supervisory dialogue that had taken place the EDPS **closed follow-up** on inspections carried out between 2017 and 2019. Responsibility for the remaining actions lies with Europol in line with the accountability principle.

iv. European Border and Coast Guard Agency, follow-up and closure of pending recommendations

In 2025, the **follow-up on the 2022 audit** on European Border and Coast Guard Agency's (Frontex) activities at EU borders was carried out. That audit had a particular focus on interviews of individuals crossing borders without authorisation and the subsequent processing of personal data. It had resulted in formulating **32 recommendations**. By May 2025, five recommendations remained pending, while ten were being addressed in the context of the ongoing formal investigation.

On 28 November 2025, EDPS **closed the audit follow-up**, considering that Frontex had adopted specific rules governing the collection of operational personal data and their transmission to Europol. The implementation of several security controls identified as necessary to mitigate data protection risks was also noted. At the

same time, Frontex remains responsible for completing the implementation of the remaining security measures.

v. European Public Prosecutor's Office audit follow-up and supervisory outcomes

In 2023, the EDPS audited the European Public Prosecutor's Office (**EPPO**) **compliance** with EU data protection law and the EPPO Regulation, focusing 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. The audit identified **11 findings** and issued **five recommendations** to enhance protection of individuals' rights, governance and storage practices within CATE. In 2024, the EPPO had implemented three recommendations and in 2025, the EDPS closed the remaining two while noting that one not implemented recommendation, risked raising non-compliance issues with the EPPO Regulation.

This highlights the need for **vigilance** and **accountability** in processing personal data in the context of criminal investigations. The EDPS's follow-up ensures that the EPPO's operational work aligns with strong data protection and fundamental rights safeguards.

9. Cooperation with the DPO Network

The Data Protection Officer (DPO) network is central to the EDPS's engagement with EUIBAs serving as a forum for **dialogue**, **collaboration** and **consistent application** of data protection rules across the EU administration. The network's **insights** help the EDPS to **better understand** practical challenges the DPOs face, and tailor supervisory guidance accordingly. In 2025, the network reinforced its dual role: as both a support mechanism and supervisory interface by integrating dialogue, guidance and enforcement. This approach strengthens DPO effectiveness and ensures uniform, rights-based data protection across EU institutions.

In 2025, the EDPS 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 practices.

In 2025, the **56th**⁴¹ and **57th**⁴² **EDPS–DPO network meetings** took place. Discussions focused on 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 avoidance of conflicts of interests. The outcomes were reflected in a new EDPS supervisory guidance⁴³.

The network functions collaboratively, with EUIBA DPOs taking turns to host the meetings. This fosters peer engagement and shared ownership. Meetings were supported by the DPO Support Group - a rotating team of volunteer DPOs who collaborated with the EDPS to develop agendas and deliver interactive sessions, including workshops and case studies.

Beyond plenary meetings, the EDPS facilitated DPO roundtables, smaller, focused discussions on key topics. In 2025, these covered the right to erasure, storage limitation, DPO independence and handling of unfounded or abusive requests.

The EDPS also issued decisions in cases involving [DPO dismissals](#), reaffirming that prior EDPS consent is mandatory and that DPO independence is a fundamental element of effective data protection governance.

⁴¹ https://www.edps.europa.eu/data-protection/our-work/publications/dpo-news/2025-07-02-56th-edps-dpo-meeting_en

⁴² https://www.edps.europa.eu/data-protection/our-work/publications/dpo-news/2025-11-27-57th-edps-dpos-meeting_en

⁴³ https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-12-18-edps-guidance-role-data-protection-officers-eu-institutions-bodies-offices-and-agencies_en

10. Data Breach Notification Management

A personal data breach is a security incident involving accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Consequences may include identity theft or reputational harm. Under the EUDPR, EUIBAs must report such breaches to the EDPS, unless the risk to individuals is unlikely.

In 2025, the EDPS received **99 personal data breach notifications**, out of which 97 admissible and two inadmissible, a nearly **11% drop from 2024**⁴⁴. Of the 97 admissible, 50 were “in phases”. The ‘in phases’ notifications are complex incidents requiring multiple actions and exchanges with the controller. By the end of 2025, the analysis of certain notifications remained pending while in one case, the EDPS identified a high risk arising contrary to EUIBA’s initial low-risk assessment. As a result, the EDPS ordered the controller to notify the affected data subjects.

While 2025 saw a slight decline in data breach notifications, new challenges emerged (e.g., interplay with AI). The EDPS handling process remains robust presenting the following results:

- 2023-2024 cases: **99% closed**.
- 2025 cases: **35% closed, 45 % on track** for closure in the first quarter of 2026.

11. Awareness raising cybersecurity exercise PATRICIA

In June 2025, the EDPS hosted the second edition of a table-top exercise titled “Personal data breach awareness In Cybersecurity Incident handling” (PATRICIA), at the EP’s Information Hub in Brussels. The event aimed to improve EUIBA staff data breach response capabilities.

The exercise brought together **35 participants** from **eight EUIBAs**, including IT managers, DPOs, and Security Officers (LISOs, LCOs), alongside the Computer Emergency Response Team of the EU Institutions, bodies and agencies (CERT-EU) as an observer. Key conclusions highlighted the need for a common understanding of responsibilities and interdisciplinary cooperation.

Following PATRICIA, the EDPS issued a **recommendations’ report**. Participants called for expanded future editions, including more EUIBAs and additional elements on personal data breach management.

By addressing gaps, EUIBAs can improve preparedness, mitigate risks and comply with EUDPR. This exercise underscored the EDPS’ role in strengthening institutional capacity, collaboration, and continuous improvement in personal data breaches management.

Legislative advisory tasks

The EDPS provides guidance on legislation proposed by the EC, which holds the exclusive right of legislative initiative, as well as to the European Parliament (EP) and the Council of the EU, which act as co-legislators. The EDPS guidance may take the form of:

- **Opinions:** issued in response to mandatory requests by the EC, which is legally obliged to seek EDPS guidance on any legislative proposal, as well as on any recommendation or proposal to the Council in the context of international agreements, where there is an impact on data protection⁴⁵.

⁴⁴ In 2024 the EDPS received 125 personal data breach notifications out of which 109 admissible and 16 inadmissible

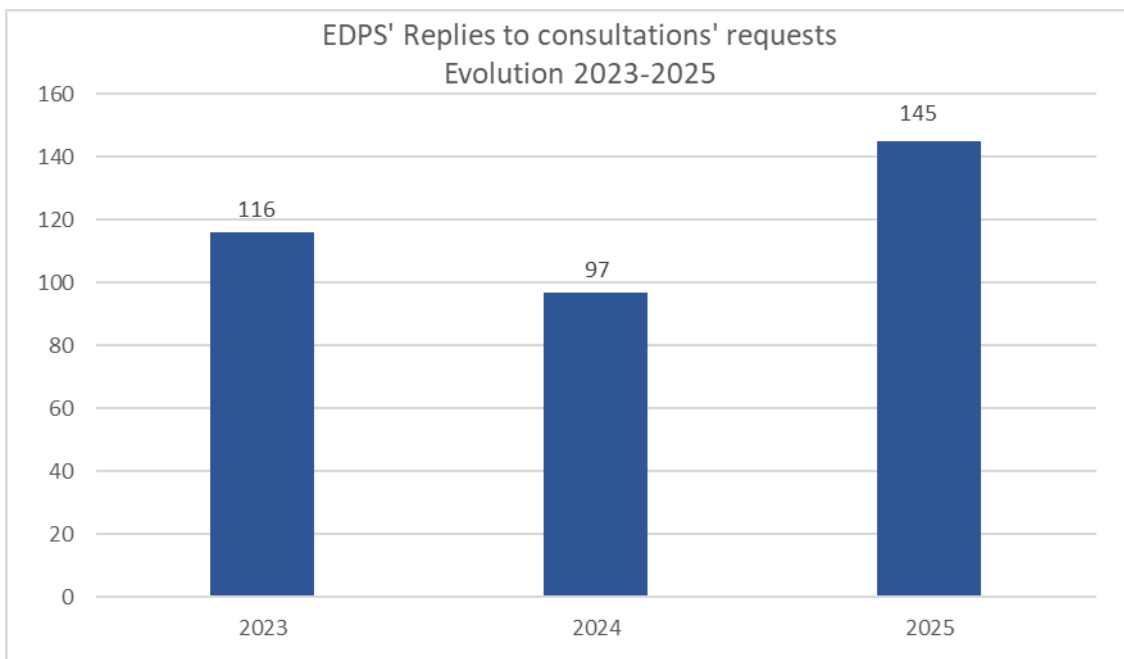
⁴⁵ Article 42(1) of EUDPR. Opinions, as well as their summaries in all official languages of the EU, are available on the EDPS website and published in the Official Journal. Opinions highlight main data protection concerns and recommendations on legislative proposals or other measures. They are issued in response to a request from the EC and are addressed to the EU co-legislator.

- Formal comments: like the opinions, formal comments are issued in response to a mandatory request from the EC, which is also legally, obliged to seek EDPS guidance when preparing delegated acts or implementing acts with an impact on data protection⁴⁶.
- Informal comments: the EC is encouraged to consult the EDPS informally before adopting a proposal, which has an impact on data protection. This allows the EDPS to provide the EC with input at an early stage of the legislative process, usually at the stage of the inter-service consultation. Informal comments are, in principle, not published.
- Joint EDPS-EDPB opinions: where a legislative or other relevant proposal is of particular importance for the protection of personal data, the EC may also consult the EDPB. In such cases, the EDPS and EDPB work together to issue a joint opinion⁴⁷.

1. Legislative consultations

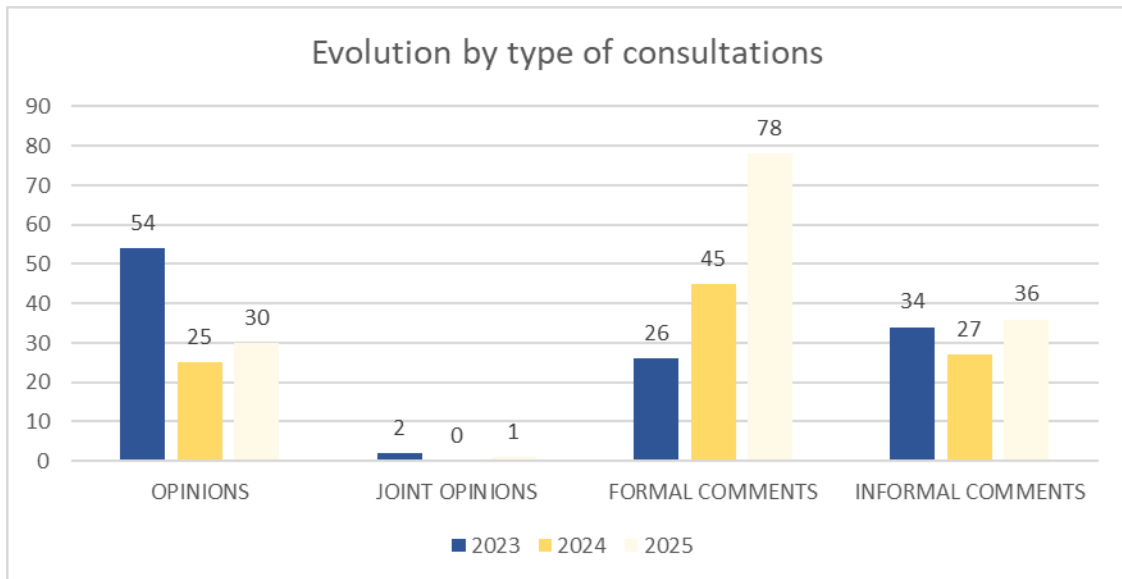
As the data protection and digital landscape continues to evolve, the EDPS' advice is increasingly sought after. The statistics indicate a growing expectation for the EDPS' involvement and advice during the informal stages of legislative and policy development.

In 2025, the EDPS responded to **145 legislative consultations** [including 108 under Article 42(1)], issued **30 opinions** and **78 formal comments**. Additionally, it provided **one EDPS-EDPB joint opinion** under Article 42(2) and **36 informal comments** and various forms of informal assistance, such as attending workshops, expert meetings, inter-service meetings, contributing to public and targeted consultations, and providing inputs for external studies and follow-up requests.



⁴⁶ Article 42(1) of EUDPR. Formal Comments are published on the EDPS website.

⁴⁷ EDPS' Rules of Procedure: https://www.edps.europa.eu/about/office-edps/edps-rules-procedure_en



2. Other advisory activities

Growing awareness of data protection issues has led to an increase in requests from the EP, its Committees⁴⁸, and individual (shadow) rapporteurs for comments or opinions on compromise amendments during trilogue negotiations. Similarly, invitations from Council working parties to present EDPS opinions have become more frequent.

To address the increasing regulatory complexity introduced by the EU's new 'Digital Rulebook', the EDPS launched in 2024 an initiative to enhance regulatory consistency and cooperation across digital economy, bringing together stakeholders from the areas of competition, consumer protection and data protection. As part of this continued effort, the EDPS published its concept note '**Towards a Digital Clearing House 2.0**⁴⁹' which encapsulates the EDPS' vision for a consistent, cooperative and coherent approach to enforcing EU laws regulating digital markets. The EDPS also published on 13 May 2025 the final version of its **Guidance**⁵⁰ for co-legislators on key elements of **legislative proposals**. The purpose of this guidance is to offer practical advice to the EC, the EP and the Council on the main elements to consider with regards to legislative proposals and other acts that imply the processing of personal data.

Advocacy and Cooperation

The EDPS is a key player and respected voice in privacy and data protection discussions. Beyond organising the Internet Privacy Engineering Network (IPEN) event for privacy engineers and monitoring technology projects that contribute to foresight debates within the EUIBAs, the EDPS actively participates in policy-making events.

In 2025, the EDPS participated in **major events**, including the Computers, Privacy and Data Protection (CPDP) conference in Brussels and the Privacy Symposium Conference in Venice.

⁴⁸ LIBE, IMCO, ECON

⁴⁹ [Towards Digital Clearing House 2.0-Concept note](#)

⁵⁰ [EDPS Guidance to co-legislators on key elements of legislative Proposals](#)

1. The EDPS as a member of the European Data Protection Board

While the EDPS is providing the EDPB Secretariat to support the EDPB activities, at the same time the EDPS is a member of the EDPB under Article 68(3) GDPR. Through **targeted** and **strategic involvement** in key EDPB initiatives, the EDPS represents the EU perspective, leveraging its expertise as the EUIBAs' supervisor. This ensures that EDPB's work is anchored in Union law, including case law of the Court of Justice of the EU, and that EDPB applies general principles of Union law.

Much of the EDPB's work is conducted within expert subgroups, each focusing on specific topics. The EDPS **coordinates** the **subgroup on** key **GDPR provisions** and actively contributes to areas such as international transfers, technology, and financial matters.

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 should be published in 2026.

As a member of the EDPB, the EDPS made significant **contributions to** various **EDPB initiatives** in 2025, including the Helsinki Statement, guidelines, comments and opinions (see details under the [EDPB dedicated section](#)). The two institutions also [jointly issued one opinion](#).

2. Cooperation with other EUIBAs and participation in Regulatory Boards

a. High-level Group for the Digital Markets Act

As a member of the High-Level Group (HLG) under Article 40 of the Digital Markets Act (DMA), the EDPS together with the EDPB, participated in its first two meetings. The HLG advises the EC and promotes a consistent regulatory approach across frameworks such as the GDPR and the ePrivacy Directive.

In 2025, the HLG endorsed a **joint paper**⁵¹ on **AI mapping** out the regulatory interplay related to AI issues. The paper also proposes to explore closer cross-regulatory cooperation among competent authorities as regards the development and deployment of AI systems by gatekeepers.

b. European Data Innovation Board

Both the EDPS and the EDPB are **members** of the European Data Innovation Board, an expert group established under Article 29 of the Data Governance Act⁵² and chaired by the EC. The tasks of this Board include **advising** and **assisting** the EC on:

- developing a consistent practice for data altruism and for the registration of data intermediation services and data altruism organisations;
- developing the European data altruism consent form;
- the prioritisation of cross-sector standards for data use and sharing between emerging common European 'data spaces' and
- guidelines for common European data spaces.

c. High-Level Group on Access to Data for Effective Law Enforcement

⁵¹ https://digital-markets-act.ec.europa.eu/document/download/f30a6d1d-8837-4b64-a385-f79969446404_en?filename=HLG%20Joint%20Paper%20on%20AI%20as%20endorsed%20on%2012%20Dec%202025.docx

⁵² <https://www.european-data-governance-act.com/>

The EDPS participated as **observer** in the High-Level Group (HLG) on Access to Data for Effective Law Enforcement, jointly established by the Presidency of the Council and the EC to explore “challenges that law enforcement practitioners in the Union face in their daily work in connection to access to data”. The HLG identified **42 recommendations** for the further development of Union policies and legislation, covering the three work strands of the HLG: digital forensics; data retention; lawful interception. Consequently, the EDPS **joined** as a member the newly established **Commission Expert Group for a Technology Roadmap on encryption**.

d. Inter-institutional Committee for Digital Transformation

The work of the Inter-institutional Committee for Digital Transformation (ICDT) is structured into various subgroups, which may further divide tasks into dedicated taskforces. The ICDT Plenary, composed of senior IT managers from all EUIBAs, meets quarterly to develop **common approaches** and oversee subgroup work. The EDPS participates on an ad-hoc basis, depending on its interests.

Beyond facilitating coordination among IT managers of EUIBAs, ICDT meetings provide valuable **insights** into **digital transformation processes** within EUIBAs, which can help shape EDPS priorities in technology monitoring and supervision. Additionally, these meetings serve as a key platform for the EDPS to communicate with IT Directors, sharing updates on supervisory activities and raise awareness of emerging technologies and their impact on privacy and data protection.

On the 17th of December 2025, the EDPS hosted the **ICDT plenary meeting**, chaired by the Court of Justice of the European Union, where the EDPS presented the closure of its investigation into the EC’s use of Microsoft 365 and the preliminary results of the mapping of possible high-risk systems in EUIBAs and Pilot project of an [AI Sandbox](#).

e. Inter-institutional Cybersecurity Board (IICB)

The EDPS is a member of the Inter-Institutional Cybersecurity Board (IICB), established under Regulation 2023/2841 (the new Cybersecurity Regulation for EUIBAs). As a guardian of lawful processing of personal data within EUIBAs, the EDPS contributes by ensuring that data security is both **robust** and **compliant** with privacy and data protection requirements. The Head of the EDPS Technology and Privacy Unit serves as the alternate to the Secretary-General, with support from the EDPS Local Information Security Officer (LISO) and Local Cybersecurity Officer (LCO).

2025 marked the first year of implementing Regulation 2023/2841. For the EDPS, this had a dual impact:

- as an EUIBA, complying with the Regulation’s demanding cybersecurity requirements, and
- as a permanent member of the IICB, acting as the cybersecurity supervisory authority for EUIBAs.

As an IICB member, the EDPS contributed to the Board’s activities, including, attending meetings and workshops, drafting and adopting guidelines, developing written procedures, and addressing Board requests for action.

f. Memorandum of understanding with the European Union Agency for Cybersecurity

Under its 2023-2025 Strategic Action Plan, the EDPS has advanced key initiatives through its Memorandum of Understanding (MoU) with European Union Agency for Cybersecurity (ENISA). The agreement strengthens collaboration on:

- cybersecurity in data protection,

- securing personal data in cybersecurity operations, and
- promoting privacy-enhancing technologies.

Key actions, include **supporting** the 2025 **Annual Privacy Forum** and participating as an observer in ENISA’s Ad Hoc Working Group on Data Protection Engineering (DPE AHWG). The EDPS considers this MoU a strategic cornerstone for effective data protection supervision across EUIBAs.

3. International cooperation

As data flow across borders, data protection should be considered in a global context. In 2025, the EDPS actively engaged in various international fora to share information and best practices, build consensus, develop guidance, and promote high data protection standards. International cooperation is facilitated through the following channels and initiatives:

a. Actions within the Memorandum of Understanding with the Spanish Data Protection Authority

The EDPS has undertaken **two key actions** under its MoU with the Spanish Data Protection Authority (AEPD), which aims to promote data protection rights, enhance cooperation, and facilitate knowledge exchange to strengthen the capacities of authorities’ technical capacities in data protection enforcement.

In June 2025, they published a TechDispatch on Federated Learning⁵³ and are currently preparing a second TechDispatch on algorithmic recommendations, set for release in early 2026.

b. Global Privacy Assembly

In 2025, the EDPS contributed to the activities of the Global Privacy Assembly (GPA), an international forum that brings together more than **130 data protection and privacy authorities** from across the globe. The GPA takes place every year. 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.

The EDPS also takes part in other GPA working groups, including the following 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; and
- data sharing.

The 2025 edition was hosted by the Personal Information Protection Commission (PIPC) of South Korea from 15 to 19 September 2025 around the theme of **‘AI in our daily lives: Data and Privacy Issues’**. The EDPS intervened in a panel for Data Protection in humanitarian action, to discuss the challenges in the age of AI and share some experiences from the cooperation with international organisations. It also intervened in a panel on developing mechanisms for collaboration among DPAs and Stakeholders.

⁵³ <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-06-10-techdispatch-12025-federated-learning>

At the occasion of this event, the GPA adopted three resolutions⁵⁴ 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 EDPS as co-sponsor
- Meaningful Human Oversight of Decisions Involving AI Systems, with 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 EUIBAs.

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.

c. Council of Europe

The EDPS participates as an observer in the Consultative Committee of the Convention 108 (T-PD), contributing to discussions and providing comments on its work. The T-PD addresses strategic data protection issues, including **AI**, oversight of **intelligence services**, **cross-border data flows**, **neurotechnology**, and **privacy enhancing technologies** (PET).

The modernised Convention 108 (Convention 108+) will enter into force once ratified by 38 parties; as of end of 2025, five ratifications were still missing for its entry into force. The EDPS continues to support the Council of Europe's (CoE) efforts to promote its **ratification**. The EDPS also represents the Global Privacy Assembly (GPA) before the T-PD, raising awareness of its initiatives and promoting alignment with EU data protection standards.

In addition, as part of the EU delegation, the EDPS contributes to the [Committee on AI](#), which developed the first-ever international legally binding convention on AI and Human Rights, Democracy and the Rule of Law, aimed at ensuring respect for human rights, democracy and the rule of law. The Committee on AI also developed the **HUDERIA methodology**⁵⁵, for assessing AI-related risks and supports its implementation capacity building initiatives and expert collaboration platforms.

d. Organisation for economic co-operation and development

The EDPS participates as both an observer and as part of the EU delegation in key working groups of the Organisation for Economic Co-operation and Development (OECD), including:

- the Working Party on Data Governance and Privacy (WPDGP), under the Committee on Digital Economy Policy, and
- the Working Party on Artificial Intelligence Governance (AIGO).

The OECD and EU share a commitment to a **human-centric, rights-based digital transformation**. The EDPS contributes to the WPDGP by providing targeted input on privacy and data protection recommendations where relevant.

⁵⁴ https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/international-conferences_fr

⁵⁵ <https://www.coe.int/en/web/portal/-/huderia-new-tool-to-assess-the-impact-of-ai-systems-on-human-rights>

The EDPS also engages with the OECD’s expert community on Data Free Flows with Trust, supporting efforts to build cross-border trust in data use. This multidisciplinary group - bringing together governments, academia, civil society, businesses, and international organisations - provides **technical expertise** to OECD policy work, with a focus on:

- cross-border payments
- legal transparency in data governance and
- privacy-enhancing technologies (PETs)

e. Cooperation with international organisations

Twenty years ago, the EDPS launched its first International Organisations Workshop - an informal yet influential **forum** where international organisations exchange **best practices**, concerns and updates on their **unique legal frameworks** and data protection **challenges**.

By 2025, the workshop was more vital than ever. With cross-border data flows accelerating - driven by humanitarian groups, global health bodies, and digital platforms, the 20th anniversary edition (25-26 September 2025, Paris) brought together **180 representatives** from **86 organisations**. Co-hosted by the EDPS and UNESCO, it focused on today’s most pressing privacy issues, including:

- safeguarding data in a shifting geopolitical landscape,
- anonymisation techniques,
- data transfers between international organisations, and
- compliance of IT tools.

Two breakout sessions, on data protection risk assessments and data subject access requests, enabled practical exchanges on building **awareness** and **accountability**. Against the backdrop of AI-driven technological and societal changes, participants explored the **impact** of AI systems in international organisations, their potential **benefits**, and **risk mitigation** strategies.

Beyond technical discussions, the workshop addressed **core values**: balancing efficiency with ethics, independence with interoperability, and security with fundamental rights. In an interconnected world, privacy protection remains critical to public trust and institutional legitimacy.

f. G7 Data Protection Authorities roundtable

The G7 DPAs roundtable convened on 18-19 June 2025, in Ottawa hosted by the Office of the Privacy Commissioner of Canada⁵⁶. The annual roundtable focused on **emerging technologies**, evolving **privacy challenges**, and the need for continued **cooperation** among like-minded authorities. A **Communiqué** and a “Statement on promoting responsible innovation and protecting children by prioritising privacy” were adopted. The protection of **children’s best interests** is particularly important with respect to the protection of children online.

In December 2025, the G7 DPAs met virtually to discuss the progress and adopted a **position paper on Data Free Flows with Trust**, highlighting the importance of regulatory cooperation to support innovation while safeguarding privacy. An Action Plan for 2026 was also endorsed, reaffirming the commitment to fostering trust and protecting privacy, particularly for children.

⁵⁶ The Group of Seven (G7) was founded in 1975 in response to the oil crisis and includes Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

g. European Conference of Data Protection Authorities

Together with EU Member States DPAs and the Council of Europe, the EDPS participated in the 33rd European Conference of Data Protection Authorities (“Spring Conference”), held on 14-16 May in Batumi, Georgia. The conference addressed **emerging trends** and **key developments** in **privacy** and **data protection**, while fostering cooperation and the exchange of best practices across Europe. The conference also adopted a Resolution on the Action Plan for Further Collaboration Activities⁵⁷.

h. High-level event on "Data-protection in the Western Balkans and Eastern Partnership Region"

Building on two fruitful events in 2023 and 2024, the EDPS hosted the 3rd high-level gathering for DPAs from the Western Balkans and Eastern Partnership in 2025. Representatives from Albania, Armenia, Bosnia and Herzegovina, Kosovo, Moldova, Montenegro, North Macedonia, Serbia and Ukraine attended a ‘Day at the EDPS’ in Brussels. The event facilitated practical **discussions** on **operational work**, **experience sharing** and accepting **common challenges**.

Key topics included:

- Best practices for advising legislators, featuring the EDPS’ Guidance for co-legislators⁵⁸
- Technology monitoring⁵⁹: challenges and solutions
- Investigative best practices, with insights from the EDPS’ supervisory work in law enforcement and border management.
- Data protection in the AI era, including the EDPS’ new supervisory role under the AI Act.

The event underscored the value of **collaborative learning**, offering insights into regional compliance challenges while reinforcing partnerships. As AI regulation and digital transformation evolve, the EDPS remains dedicated to strengthening cooperation, enhancing privacy protections, and shaping global data protection standards.

i. Strasbourg EDPS office

In 2022, the EDPS established a permanent Strasbourg office to **strengthen** its **inter-institutional** and **international engagement**.

The office supports three key objectives:

- Deepening ties with the Council of Europe (CoE), a vital partner in European and global data protection;
- Monitoring EP activity, particularly plenary sessions where key data protection legislation is debated, and
- Enhancing cooperation with EUIBAs based in Strasbourg, such as eu-LISA.

Its presence enables the EDPS to attend EP and CoE events and hold informal discussions. Strengthening these connections remains a core focus of the Strasbourg office.

⁵⁷ https://www.edps.europa.eu/system/files/2025-05/adopted-resolution-08052025_en.pdf

⁵⁸ https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-05-07-guidance-co-legislators-key-elements-legislative-proposals_en

⁵⁹ https://www.edps.europa.eu/data-protection/technology-monitoring_en

j. International Working Group on Data Protection in Technology (the Berlin Group)

The EDPS actively participates in the International Working Group on Data Protection and Technology, known as the Berlin Group. This Group constitutes a global forum for DPAs, independent experts from public bodies, private organisations, academia, and civil society. The Berlin Group **assesses emerging technologies** and promotes **privacy-enhancing solutions** for data-driven services.

In 2025, the EDPS contributed to **two** Berlin Group **meetings**, one held in Tbilisi, Georgia, and one in Montevideo, Uruguay. Discussions included working papers on Global opt-out preference signals and related technologies, Extended Reality and Confidential Cloud Computing (with the EDPS contributing as co-rapporteur).

Technology monitoring tasks

Technology Monitoring is a core EDPS responsibility under Art. 57(h) of the EUDPR, enabling the organisation to assess the impact of technological developments on data protection and anticipate future trends. In 2025, the EDPS boosted its technological assessment and digital innovation capabilities, analysing emerging trends, while maintaining active engagement with the public and privacy experts in a fast-evolving digital landscape.

a. TechSonar

In November 2025, the EDPS released its 5th TechSonar report, **analysing emerging technological trends** and their data protection **implications**.

The 2025-2026 edition⁶⁰ focused on six AI-driven developments:

- Agentic AI
- AI companions
- Automated proctoring
- AI-driven personalised learning
- Coding assistants
- Confidential computing

Each trend was examined through a technology overview, development trends, and individuals. The report for each trend concludes with recommended reading for deeper exploration and recorded podcast series (one per trend).

b. TechDispatch

While TechSonar provides an initial overview on technology trends, TechDispatches **delve deeper** into **emerging technologies** and their **impact**. In 2025, the EDPS published **three** TechDispatches:

1. The Federated learning⁶¹, in collaboration with the Spanish Data Protection Authority (AEPD), is a privacy-preserving machine learning approach particularly valuable in healthcare and autonomous transport systems.

⁶⁰ https://www.edps.europa.eu/data-protection/our-work/publications/reports/2025-11-24-techsonar-2025-2026_en

⁶¹ <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-06-10-techdispatch-12025-federated-learning>

2. The human oversight of automated decision making⁶², which examines how to ensure human control over AI systems while upholding democratic values and human rights.
3. The Digital Identity Wallets (DIW)⁶³, which assess privacy risks and EU compliance, including the European Digital Identity Wallet.

The first two TechDispatches were paired with a TechDispatch Talk (video podcast) and the third with a video.

c. Internet Privacy Engineering Network (IPEN)

The IPEN initiative, founded by the EDPS in 2014, drives privacy engineering best practices. Its annual events, often linked to ENISA's Annual Privacy Forum, explore **cutting-edge solutions**.

For 2025, the focus was 'Secure multi-party computation' (SMPC), a breakthrough for privacy-preserving data processing in domains such as **finance** and **healthcare**. Co-hosted with the Goethe University Frankfurt in October 2025, the IPEN event⁶⁴ brought together **experts** from academia, industry, and technology to examine SMPC's growing role in tackling data privacy, digital sovereignty, and cross-border data collaboration challenges.

The next IPEN event is scheduled for September 2026 in Salzburg, Austria.

d. EDPS AI risk management guidance

In November 2025, the EDPS issued new guidelines with practical recommendations to help **identify** and **mitigate common** technical **risks** in AI systems⁶⁵. Aimed at EUIBAs acting as controllers, the guidelines focus on key data protection principles, including fairness, accuracy, data minimisation, security and data subjects' rights.

e. Website Compliance Awareness Campaign (WCAC)

EUIBAs manage over **1 300 websites**, making individual audits impractical given the EDPS' limited resources. To improve compliance efficiently, the EDPS launched the WCAC to raise awareness of potential issues and support controllers in meeting their accountability obligations.

In 2018, the EDPS developed the **Website Evidence Collector (WEC)** tool for remote website audits and made it publicly available to help controllers and DPOs identify and address website compliance gaps. However, its use among EUIBAs remains limited. During the WCAC pilot phase, the EDPS used WEC to check one website per EUIBA every 6 months (over 70 in total). Three scan waves were rolled out, in October 2024, in April 2025 and in October 2025 respectively. Inclusion in the campaign does not preclude EDPS supervisory action, including investigations.

⁶² <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-09-23-techdispatch-22025-human-oversight-automated-making>

⁶³ <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-12-15-techdispatch-32025-digital-identity-wallets>

⁶⁴ Recordings of the IPEN event on "Secure multi-party computation" available at: https://www.edps.europa.eu/data-protection/technology-monitoring/ipen/ipen-event-secure-multi-party-computation_en

⁶⁵ https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-11-11-guidance-risk-management-artificial-intelligence-systems_en

In 2025, the EDPS shared **factual reports** with the concerned EUIBAs for each website and scan wave. These reports help EUIBAs to identify and **assess** data protection **weaknesses** - particularly under Article 37 EUDPR, and Article 5(3) ePrivacy Directive - and support corrective actions.

Following the pilot phase, the EDPS is assessing how to **scale the campaign** more efficiently to cover a larger share of the 1 300+ EUIBAs' websites.

Artificial Intelligence

The Artificial Intelligence (AI) Act⁶⁶ broadened EDPS' role, entrusting it with:

- the **Market Surveillance Authority (MSA)**, overseeing AI systems used by EUIBAs, and
- **Notified Body**, testing and inspecting 'high-risk' AI systems deployed by EUIBAs to ensure compliance.

Preparedness for supervision and enforcement

Ahead of the August 2026 deadline for the entry into force of high-risk AI provisions under the AI Act, the EDPS intensified preparations for undertaking its role as MSA and Notified Body effectively and efficiently. In 2025, efforts focused on building the organisational, analytical and procedural foundations for effective supervision of AI systems across the EU public administration.

a. Consolidating the AI unit

A key priority in 2025 was consolidating the AI unit, integrating legal, technical, and policy expertise to move from strategic preparation to concrete supervisory action. Technical and procedural steps were advanced, alongside investment in human and technical expertise, to ensure that the **EDPS keeps pace with a rapidly evolving AI landscape**. Institutional capacity was further strengthened in AI technologies, data and computing, health and safety risks, and applicable standards and legal requirements, in line with Article 70(3) of the AI Act.

b. Mapping

Effective AI supervision requires a **clear understanding** of its use across EUIBAs. In 2025, the EDPS conducted a mapping exercise identifying around 186 AI systems in use or planned, with finding published in a dedicated report⁶⁷.

The exercise shows that EUIBAs are primarily users rather than developers, relying largely on externally developed, off-the-shelf AI tools. This underscores that **accountability** for deployment and use remains with EUIBAs, including where systems are procured from third parties.

It also highlights the growing uptake of generative AI, alongside a significant number of systems still in pilot or development phases, including active exploration coupled with the **gradual build-up** of internal **expertise and governance**.

⁶⁶ [Regulation \(EU\) 2024/1689](#) of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)

⁶⁷ https://www.edps.europa.eu/data-protection/our-work/publications/ai-act/2025-12-04-high-risk-ai-systems-mapping-report-european-institutions-agencies-and-bodies_en

Finally, higher-impact AI systems are more likely to be deployed in **sensitive areas** such as migration, law enforcement and employment. By clarifying where such systems arise, the mapping helps demystify ‘high-risk’ AI and reinforces that these systems are not prohibited but require robust governance and oversight.

c. Developing internal procedures

Building on the mapping exercise and legal analysis, the EDPS moved **from assessment to operational readiness**, shifting focus to hands-on supervision under the AI Act.

To prepare for the use of the MSA powers, including under the Market Surveillance Regulation, internal **procedures** were developed and organisational structure adjusted. These changes support the transparent, independent operationalisation of the new EDPS role, while establishing a coherent supervisory framework that enhances legal certainty and reduces compliance risk for AI systems used by EUIBAs.

Work also advanced on ensuring functional separation between the EDPS’ **roles** under the EUDPR and its responsibilities as a MSA and Notified Body under the AI Act. This distinction is essential for effective oversight, coordination with the authorities protecting fundamental rights, and clear enforcement procedures, including complaints handling.

In parallel, the EDPS closely monitored the development of **harmonised standards** under the **AI Act**, which will be critical for translating legal requirements into practice. Anticipating these standards supports clearer guidance to EUIBAs and reduces uncertainty during implementation.

Institutional Empowerment

In 2025, the EDPS continued to prioritise institutional empowerment, ensuring that EUIBAs are not only aware of their obligations under the AI Act but also equipped with the **knowledge, tools, and networks** to implement them effectively. This objective was advanced through **two key initiatives**: the AI Act Correspondent Network and the AI regulatory sandbox pilot project.

a. The AI Act Correspondent Network

The central pillar of the EDPS’ institutional capacity-building was the development of the AI Act Correspondent Network (AIACN), established in 2024 and inspired by international governance models and the DPO network. Each EUIBA voluntarily appointed representatives with legal, technical, and policy expertise to participate in its activities.

The AIACN serves as a hub for **compliance support, capacity-building and knowledge exchange** on AI governance. In 2025, it also operated as a forum for sharing best practices, coordination and mutual learning as EUIBAs prepared for the AI Act.

Two AIACN meetings were held in Brussels. The first⁶⁸ meeting in January 2025 focused on AI Act preparedness, covering the implementation timeline, key roles and the involvement of supervisory authorities.

⁶⁸ https://www.edps.europa.eu/press-publications/press-news/blog/1st-meeting-ai-correspondents-network-community-compliance-and-collaboration_en

The second⁶⁹ meeting, held in October 2025, advanced these discussions with expert input on fundamental rights impact assessments, updated guidance from the EC's AI Office, and the presentation of preliminary findings from the EDPS' mapping of AI systems, enabling EUIBAs to benchmark their practices within the broader administrative landscape.

b. The AI regulatory sandbox

In 2025, the EDPS prepared a pilot AI regulatory sandbox, in the context of the 2nd meeting of the AIACN, to support EUIBAs in preparing for the AI Act, to be rolled out in 2026. The initiative addresses the need to **reconcile innovation** with **compliance** as the use of AI is growing under legal and technical uncertainty.

The sandbox provides a **controlled testing environment** in which EUIBAs can develop, test, and validate AI systems prior to deployment. The EDPS offers tailored regulatory guidance while ensuring compliance with fundamental rights and safety requirements. Early testing under supervisory conditions helps identify and address compliance risks at an early stage, reducing the need for costly adjustments later.

This pilot reflects the evolving regulatory context, with EDPS enforcement powers under the AI Act applying from August 2026, alongside provisions on regulatory sandboxes. Ahead of this date, the pilot project will provide a cooperative space for experimentation and mutual learning and will enable EUIBAs to reflect on concrete AI use cases.

Participation to the pilot project is voluntary and designed as an opportunity for EUIBAs to engage proactively in AI Act readiness. At the same time, it supports the EDPS understanding of institutional needs and challenges, in view of establishing an official regulatory sandbox.

Legislative and Policy Analysis

The EDPS contributed to shaping the interpretation and application of the AI Act within the EU public sector, including key framework documents supporting its implementation. Its legislative and policy analysis aims at ensuring that the AI Act is translated into guidance and processes that are **legally** sound, operationally **feasible**, and **aligned** with **fundamental rights** and product **safety** requirements.

a. AI Board

The EDPS participates as an observer to the AI Board, an advisory and coordination body established by the AI Act to ensure consistent implementation, and enforcement across EU Member States. In this role, the EDPS contributes to the AI Board and its sub-groups **discussions** (including standards, high-risk systems, prohibitions, and law enforcement), as well as **consultations** and supporting documents.

This engagement enables the EDPS to highlight its role within the **AI governance framework** and to share relevant insights with EUIBAs, supporting timely compliance. It also contributes to a **consistent interpretation** of the AI Act, helping anticipate future guidance and informing EDPS's supervisory approach.

⁶⁹ https://www.edps.europa.eu/press-publications/press-news/blog/building-collaboration-second-meeting-ai-act-correspondents-network_en

b. Analysing the AI Act

The EDPS conducted extensive legal analysis of the AI Act, focusing on its application to EUIBAs and its interaction with other legal frameworks, including data protection and EUIs-specific rules. This early and in-depth work helped anticipate **interpretative challenges** and promote **legal certainty** for EUIBAs preparing for compliance.

This analysis also identified practical implications for the EDPS, supporting alignment of its organisational set-up and procedures with the new legal framework. Overall, it helped bridge the gap between legislation and practice, strengthened the EDPS's preparedness, and laid the groundwork for consistent, proportionate, and effective supervision of AI systems in the EU public sector.

Cooperation with national market surveillance authorities

The EDPS strengthened cooperation with national market surveillance authorities (MSAs), notably through its participation as a full member of AI Board's standing subgroup on market surveillance, which serves as the Administrative Cooperation Group (ADCO) for the AI Act. This engagement was key in 2025 to support **consistent supervision**, effective **information-sharing**, and a **coherent application** of the AI Act across Member States, avoiding fragmented oversight.

International engagement and exchange of best practices

Recognising the cross-border nature of AI governance, the EDPS, in its role as MSA and Notified Body, ensured active participation in international institutions and networks, contributing expertise and promoting the exchange of supervisory and enforcement practices.

The EDPS participated to **initiatives** such as the:

- Global Network of AI Supervisory Authorities (GNAIS), led by UNESCO, as a full member, working with other supervisors on assessment frameworks, methodologies and supervisory tools;
- Council of Europe, including work on the methodology for the risk and impact assessment of AI systems from the point of view of Human Rights, Democracy and the Rule of Law (HUDERIA methodology); and
- activities of the Organisation for Economic Co-operation and Development's Artificial Intelligence Policy Observatory (OECD.AI) and its Global Partnership on Artificial Intelligence.

It also engaged with **research initiatives** supporting evidence-based policymaking, such as the NoLeFa project, which brings together public bodies, SMEs, startups, and research networks to support market surveillance through testing, coordination, and standardisation.

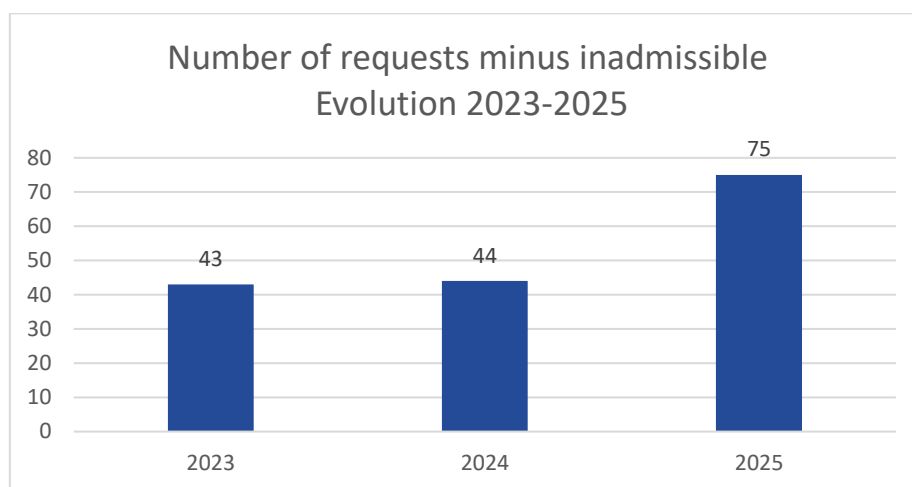
Additionally, the EDPS shared expertise through participation in international events and collaboration with technical experts and academia.

Data Protection Officer Activities

In 2025, the Data Protection Officer (DPO) collaborated with responsible services to strengthen the EDPS' data protection compliance and accountability.

The DPO monitors the practical application of data protection rules under EUDPR, case law and relevant guidance. The EDPS' register of personal data processing activities was regularly updated, and new or revised data protection notices were made available to enhance transparency for data subjects.

In 2025, the DPO processed **75 data subjects' requests**⁷⁰ (excluding inadmissible requests) representing a **70% increase** in these requests. In certain cases, individuals exercised more than one data protection right, such as access and erasure requests.



The DPO also assisted in handling **11 personal data breaches**. Due to the low risk to natural persons' rights and freedoms, ten did not require notification to the supervisory authority, while one was reported and mitigated accordingly.

In 2025, the DPO delivered training and awareness raising activities on data protection, including sessions for new EDPS staff members.

Collaboration with other EUIBAs' DPOs continued through regular meetings and working groups, including biannual network meetings in July and November (see as well [DPO network](#)). For strengthening cooperation between the EDPS and the EUIBAs' DPOs, three EDPS-DPOs roundtables were held, fostering discussions around data protection rules and how individuals' personal data are adequately protected according to the EU's values and principles.

Access to documents

According to Article 52(4) of the EUDPR and to the EDPS Rules of Procedure, the organisation is subject to Regulation 1049/2001 on public access to documents⁷¹. For each request submitted to the EDPS, the Transparency officer collaborates with the relevant services for responding appropriately to the request.

In 2025, the EDPS received **72 access to documents requests**, representing an **increase of 36%** compared to the previous year. Out of these 72 requests, **11**⁷² were **confirmatory applications** (appeals). In 11 cases access to the documents falling within the scope of the request were denied as they were covered by exceptions⁷³. In all other cases where documents could be identified, they were either fully or partially disclosed to the applicant.

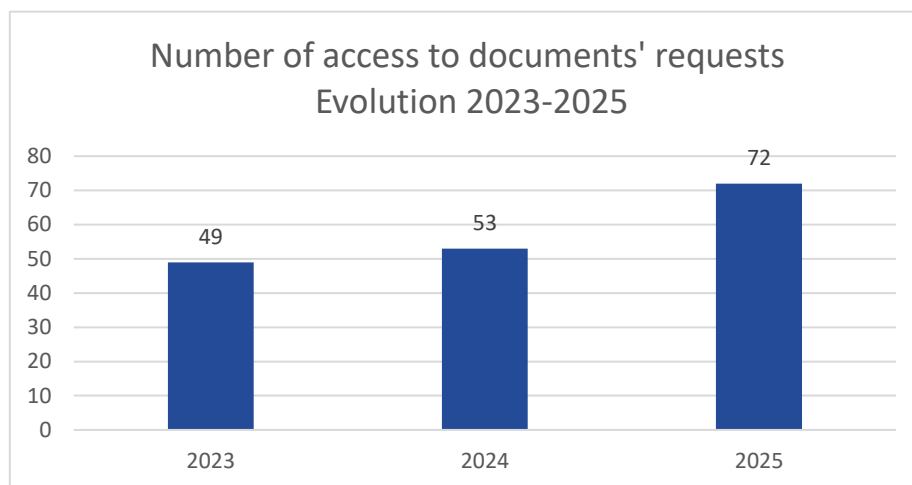
⁷⁰ More specifically, the EDPS replied to 30 access requests, 27 erasure requests, 7 information requests, 1 rectification request, 1 objection request, 2 consent withdrawals, 7 allegations of personal data breaches (that were ultimately not confirmed as breaches) and 67 inadmissible requests. It should be noted that all 67 inadmissible requests are equally analysed by the EDPS as the rest of the queries and each one received a response.

⁷¹ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents: <https://eur-lex.europa.eu/eli/reg/2001/1049/oj/eng>

⁷² Representing ~15% of all cases in 2024.

⁷³ Exceptions of Article 4(1)(a), (2) and (3) of Regulation (EC) No 1049/2001.

The EDPS remains fully committed to increasing transparency and accountability of the work done and aims to update the website, and the public register in particular, with relevant documents and information on a regular basis.



Communication

Transparent, accessible communication remains at the core of the EDPS' mandate. In 2025, the EDPS stepped up outreach on data protection and artificial intelligence (AI), ensuring its work is clear, relevant, and widely accessible.

The EDPS sustained a **strong, diversified** online **presence** across its **website** and **social media**, using targeted content to drive visibility and engagement.

Key communication channels, with a total of **over 129 000 subscribers**, included:

- X, highlighting participation in events, key decisions and institutional updates.
- LinkedIn, the EDPS primary professional channel and fastest-growing platform, engaging privacy, data protection and AI specialists, stakeholders and prospective candidates.
- Instagram, providing accessible and interactive content, particularly for younger audiences.
- YouTube, hosting event recordings, awareness-raising videos, employer branding video campaign and episodes of the "EDPS on Air" podcast, to name a few.
- Mastodon, reactivated in 2025 to support a decentralised and privacy-friendly social media presence.

Targeted **campaigns** throughout the year included:

- #InCaseYouMissedIt, drawing renewed attention to key but less visible activities.
- European Cybersecurity Month, promoting responsible AI deployment and cybersecurity awareness.
- Monthly Recaps, highlighting Opinions, guidance and major publications.
- 'Myths Busted', addressing common misconceptions about data protection and citizens' rights.

The **EDPS website** remained its central hub for press releases, opinions, comments, newsletters, podcasts and blog posts, with technical upgrades in 2025 improving accessibility and user experience.

Media engagement remained strong. In 2025, the EDPS issued **12 press releases** on major enforcement actions, policy contributions and guidance, alongside interviews, press conferences, responses to media inquiries, and timely responses to public inquiries.

Events and stakeholder engagement were a continued priority. In 2025, the EDPS contributed to and organised major initiatives, including, among others, Computers, Privacy and Data Protection (CPDP) – Data Protection Day, the annual CPDP Conference, the High-Level Debate on Competition, Innovation and Data Protection, the PATRICIA II exercise on personal data breaches, the International Organisations Workshop on

Data Protection (co-hosted with UNESCO), EU Open Day, and the “From Cradle to Cloud” conference on children’s digital rights. The EDPS also organised **nine study visits**, welcoming **194 participants** to its Brussels and Strasbourg offices.

Employer Branding was further reinforced. A key milestone was the redesign of the **EDPS Careers page**. Campaigns such as #teamEDPS – Join us and Meet #teamEDPS showcased career opportunities, staff stories, and traineeships, primarily via LinkedIn and Instagram.

Secretariat of the European Data Protection Board

The Secretariat of the European Data Protection Board (EDPB) offers analytical, administrative and logistical support to the EDPB. The Secretariat is composed of five sectors (a sector for legal affairs -cooperation and enforcement, a sector for litigation and international affairs, an information and communications sector, an IT sector and an administrative sector).

In line with the Article 75 of the GDPR, staff at the EDPB Secretariat is employed by the EDPS and works under the instructions of the Chair of the EDPB. The terms of cooperation between the EDPB and the EDPS are established by the Memorandum of Understanding. While the EDPS employs the staff at the EDPB Secretariat, they work exclusively under the instructions of the Chair of the EDPB. In 2025, the budget of the EDPB covers **47 staff members** who work within the EDPB Secretariat or within the EDPS for the support provided to the EDPB via horizontal administrative services.

The EDPB budget forms part of the broader EDPS budget. For 2025, the adopted budget of the EDPB amounted to EUR 8 823 million. This budget supports the growth of enforcement and litigation activities and covers expenditure for EDPB meetings at the plenary and subgroup level, translation and interpretation costs, IT services, and remuneration of the EDPB Secretariat staff.

Support to the EDPB activities

The EDPB Secretariat plays a key role in the preparation and execution of many of the tasks entrusted to the EDPB, and thus in **harmonising** the **guidance**, **procedures**, enforcement **processes** and **practices** of Data Protection Authorities (DPAs) across Member States.

Helsinki statement

At a high-level meeting in Helsinki on 1–2 July 2025, the European Data Protection Board (EDPB) adopted a landmark [Statement on enhanced clarity, support and engagement](#).

The Statement outlines new initiatives to make GDPR compliance **easier**, in particular for **micro, small and medium organisations**, strengthen **consistency**, boost cross-regulatory **cooperation**, and enhance the EDPB **dialogue** with stakeholders. The statement reflects the EDPB efforts to reduce the administrative burden for businesses, while ensuring the protection of individuals’ fundamental rights.

Binding decisions

In 2025, **no binding decisions** were adopted by the EDPB. This shows progress in **building consensus** and cooperation among DPAs. The consistent dialogue facilitated by the EDPB has allowed DPAs to resolve cases more efficiently at the national level, contributing to a harmonised enforcement landscape across Europe.

Consistency opinions

DPA's may seek consistency opinions from the EDPB under Article 64 (1) GDPR, addressed to DPA's, including: opinions on draft decisions regarding Binding Corporate Rules, opinions on draft requirements for the accreditation of a certification body, opinions on certification criteria and opinions on DPA's approval of accreditation requirements for a code of conduct monitoring body. DPA's must take the utmost account of the consistency opinion when finalising their national decisions.

In 2025, the EDPB adopted **29** Article 64(1) GDPR **opinions**, reflecting its continued commitment to promoting harmonisation. **Since** its establishment in **2018**, the EDPB has issued **a total of 217** Article 64(1) **opinions**, demonstrating the sustained importance of this mechanism in supporting a harmonised application of the GDPR.

The EDPB may also prepare consistency opinions under Article 64(2) GDPR on matters of general application or those with significant cross-border implications. Such opinions can be requested by the EDPB Chair, DPA's, or the EC to address broad, recurring issues or complex legal questions, ensuring alignment across Member States. These opinions help avoid conflicting DPA's decisions and ensure that the GDPR rules are applied consistently in the EU. In 2025, the EDPB did not adopt any Article 64(2) GDPR opinion.

General guidance

One of the EDPB's core competences is to clarify the GDPR by issuing guidance. As such, the EDPB established a well-defined and comprehensive repository of guidelines and recommendations, which continues to expand. This ensures that DPA's apply data protection laws **consistently** and it further strengthens stakeholder **compliance**. The EDPB makes a consistent effort to incorporate stakeholder input, which is collected via **public consultation** and the organisation of stakeholder events on dedicated topics.

In 2025, the EDPB adopted **three new guidelines**, namely: 1) [guidelines 01/2025 on pseudonymisation](#), 2) [guidelines 02/2025 on processing of personal data through blockchain technologies](#), and 3) [guidelines 3/2025 on the interplay between the DSA and the GDPR](#). The EDPB also adopted the final version of [guidelines 02/2024 on Article 48 GDPR](#) following public consultation.

In addition, the EDPB and the EC endorsed [joint guidelines on the interplay between the Digital Markets Act \(DMA\) and the GDPR](#). The DMA and the GDPR both protect individuals in the digital landscape, but their goals are complementary as they address **interconnected challenges**: individual rights and privacy in case of the GDPR and fairness and contestability of digital markets under the DMA. These are the first joint guidelines by the Board and the EC. This approach maximises usefulness of the guidance by simplifying compliance for businesses and bringing enhanced legal certainty to them.

The Board also adopted **two sets of recommendations**: [recommendations 1/2025 on the 2027 WADA World Anti-Doping Code](#) and [recommendations 2/2025 on the legal basis for requiring user account creation on e-commerce websites](#).

Legislative consultation

The EDPB advises the EC on data protection issues and any proposed new EU legislation of particular importance for the protection of personal data. In the context of legislative consultations requested by the EC, the EDPB adopts opinions on issues pertaining to data protection in the EU, which may be adopted solely by the EDPB or jointly with the EDPS. The EDPB may also advise the EC on the assessment of the adequacy of the level of protection in a third country.

a. Statements

In 2025, the EDPB issued **three** statements: 1) [statement 1/2025 on age assurance](#), 2) [statement 2/2025 on the implementation of the PNR Directive in light of CJEU Judgment C-817/19](#) and 3) [statement 4/2025 on the EC's Recommendation on draft non-binding model contractual terms on data sharing under the Data Act](#).

b. Opinions on adequacy decisions

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

In 2025 the EDPB provided **five opinions** on the adequacy of personal data protection:

- [Opinion 06/2025 regarding the extension of the EC Implementing Decisions under the GDPR and the LED on the adequate protection of personal data in the United Kingdom \(Art.70\(1\)\(s\) GDPR and Art. 51\(1\)\(g\) LED\)](#)
- [Opinion 07/2025 regarding the EC Draft Implementing Decision pursuant to Regulation \(EU\) 2016/679 on the adequate protection of personal data by the European Patent Organisation \(EPO\) \(Art.70\(1\)\(s\) GDPR\)](#)
- [Opinion 26/2025 regarding the EC Draft Implementing Decision pursuant to Regulation \(EU\) 2016/679 on the adequate protection of personal data by the United Kingdom](#)
- [Opinion 27/2025 regarding the EC Draft Implementing Decision pursuant to Directive \(EU\) 2016/680 on the adequate protection of personal data by the United Kingdom \(Art. 51\(1\)\(g\) LED\)](#)
- [Opinion 28/2025 regarding the EC Draft Implementing Decision pursuant to Regulation \(EU\) 2016/679 on the adequate protection of personal data by Brazil \(Art. 70\(1\)\(s\) GDPR\)](#)

Enforcement cooperation

As part of its [strategy](#), the EDPB supports efficient **functioning** of the **cooperation** and **consistency mechanism** linking all national supervisory authorities, which work together to enforce European data protection law, by streamlining internal processes, combining expertise and promoting enhanced coordination.

Several programmes have been launched to this end. The EDPB Secretariat has a leading role in implementing and coordinating the following programmes:

a. The Support Pool of Experts

The Support Pool of Experts (SPE) has continued to play a key role in strengthening the enforcement capacity of DPAs. This initiative, part of the EDPB's Strategy 2024-2027, provides **critical technical expertise** and **tools** to address complex cases and emerging data protection challenges. In 2025, **nine projects** have been launched to enhance GDPR compliance and enforcement across the EU. Since their last annual report, the EDPB published the deliverables of **seven SPE projects**.

The published SPE projects included **six new reports**, a new version of the Website Auditing Tool (WAT) as well as a video tutorial for the WAT.

One major project involved creating a [case digest on the right of access](#). This initiative provides DPAs with a consolidated repository of decisions, offering valuable insights into recurring issues and thematic trends in enforcement.

Another notable project was the launch of a new version of the [EDPB Website Auditing Tool](#) which helps analyse whether websites are compliant with the law. The new tool allows the preparation, completion and

evaluation of audits directly in the tool by a simple visit to the website concerned. In 2025, the EDPB had **two parallel projects** to improve the software and its adoption: a new version of the software and a video tutorial of the website auditing tool.

The other SPE projects published in 2025 include [AI: Complex Algorithms and effective Data Protection Supervision](#), [AI Privacy Risks & Mitigations Large Language Models \(LLMs\)](#), and [The Digital Euro and its token-based offline modality](#).

Two training curriculum on **AI** and **data protection** were also developed: [Law & Compliance in AI Security & Data Protection](#) and [Fundamentals of Secure AI Systems with Personal Data](#).

In addition to these initiatives, the EDPB organised a **Bootcamp** covering the topics of **AI** and **AI Auditing** in October 2025, which built on the success of previous bootcamps. The event brought together 50 participants from 24 countries, and the EDPS, for a series of expert-led sessions, workshops and trainings.

b. Taskforce on Generative AI Enforcement

In 2025, the rapid advancements in artificial intelligence (AI) prompted the EDPB to extend the mandate of the ChatGPT taskforce, focusing on fostering cooperation and exchanging information on enforcement relating more broadly to AI. The taskforce on Generative AI Enforcement helps **enhance cooperation** among DPAs on enforcement activities and **ensure compliance** with the GDPR.

c. Quick Response Team

In 2025, the Board decided to launch a pilot project consisting of the creation of a quick response team to facilitate DPAs' coordination regarding **urgent sensitive matters**.

d. The Coordinated Enforcement Framework (CEF)

In 2025, the EDPB launched its coordinated enforcement action on the right to erasure or the “right to be forgotten” (Article 17 GDPR), as it is one of the most frequently exercised GDPR rights and one about which DPAs frequently receive complaints from individuals.

32 DPAs across Europe took part in this initiative. Participating DPAs contacted more than **700 controllers** from different sectors across Europe, either by opening new formal investigations or doing fact-finding exercises. In the latter case, they may also decide to undertake additional follow-up actions if needed.

DPAs checked how controllers handle and respond to the requests for erasure that they receive, and in particular, how they apply the conditions and exceptions for the exercise of this right. DPAs stayed in close contact to share and discuss their findings throughout the year.

The **results** of these national actions are aggregated and analysed together in a consolidated [EDPB report](#) to generate deeper insights into the topic, allowing for targeted follow-ups on both national and EU levels.

Litigation

In 2025, the EDPB was involved as a party in **15 cases before the Court of Justice of the European Union** (CJEU), one of which was submitted in 2022, ten in 2023, two in 2024, and **two in 2025**. In addition, in 2025, the EDPB was involved **as intervener in one case**, in support of the EDPS. During all proceedings, the Secretariat of the EDPB collaborated closely with external lawyers at every stage. This included defining the

EDPB's legal strategy, drafting procedural documents, and preparing for and attending hearings before the CJEU.

Coordinated Supervision Committee

The Coordinated Supervision Committee (CSC) is a group of national DPAs and the EDPS. It ensures coordinated **supervision of large-scale IT systems** and of **EUIBAs**, in accordance with Art. 62 of EUDPR or with the EU legal act establishing the large-scale IT system or the EUIBA. These also include the Schengen information system (SIS), the Visa Information System (VIS), the Internal Market Information System (IMI), the Customs Information System, the European Union Agency for Criminal Justice Cooperation (Eurojust), and the European Union Agency for Law Enforcement Cooperation (Europol).

The CSC also provides a forum for **cooperation** in the context of the European Public Prosecutor Office (EPPO), the prosecution body responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget.

The EDPB Secretariat provides the Secretariat of the CSC and offers **analytical, administrative and logistical** support. This support includes preparation of positions, organising CSC meetings and communication.

In 2025, the CSC published its [biannual activity report \(July 2022 - December 2024\)](#), its [Annual Report 2023 of SIS Statistics](#), and its [work programme 2025-2026](#). On the occasion of the entry into operation of the EU Entry Exit System on 12 October 2025, the Coordinated Supervision Committee included it under its scope.

Data Protection Officer Activities

The EDPB processes personal data according to the rules laid down in the EUDPR. In accordance with Article 43 of this Regulation, the EDPB has its own Data Protection Officer (DPO). In 2025, the EDPB received **12 individual requests** based on rights under Article 17 to Article 24 EUDPR. The EDPB Secretariat also provided assistance with replying to individual **requests for information** involving the processing of their personal data and supported in handling nine personal data breaches, one of which required a notification to the EDPS.

Access to documents

In accordance with Article 32 (2) of the EDPB Rules of Procedure (RoP), the EDPB Secretariat prepares the answers to access requests to EDPB documents. Initial requests are handled and signed by one of the Deputy Chairs. Confirmatory requests are handled and signed by the Chair. In 2025, the EDPB Secretariat received **20 public access requests** for documents held by the EDPB. **Confirmatory applications** were received in **six cases**. The EDPB also received **five consultation requests** from EDPB members on national access to document requests concerning documents originated from the EDPB. No complaint regarding the EDPB confirmatory decisions for an access to documents request was brought to the attention of the European Ombudsman in 2025.

Communication, Information Technology & Administration

The EDPB provides IT solutions to ensure secure and transparent communications between all the European National DPAs, handles media relations, and organises meetings.

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

To this end, the EDPB Secretariat took the lead in the launch of a series of visual attractive **summaries** to explain EDPB guidance to the general audience in an easier and more understandable way. This was an important **awareness raising action** in 2025. The main objective of these summaries is to help organisations understand the key points to consider for ensuring compliance with the GDPR. Following the initial summary on [the Guidelines 1/2024 on processing of personal data based on Article 6\(1\)\(f\) GDPR](#) at the end of 2024, the EDPB published **five additional summaries in 2025**, covering: [pseudonymisation](#), [personal data breaches](#), [blockchain technologies](#), [right of access](#) and the [interplay between the Digital Services Act \(DSA\) and the GDPR](#).

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

In 2025, the Secretariat successfully addressed **over 800 support requests** concerning the IMI system and efficiently handled a total of 10.481 inquiries across all EDPB IT systems, delivering prompt and effective assistance to stakeholders.

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

The **EDPB HUB** maintained its pivotal role as the premier platform for internal communication and information dissemination in 2025. With **over 10 000 content pieces** created and shared, the platform saw a substantial increase in activity compared to past years. The EDPB Secretariat also ensured the continued usability of the EDPB website, which attracted **317 187 visits** and recorded **1 516 687 page views** throughout the year. The EDPB Secretariat also organised over **500 meetings**.

In December 2025, the EDPB Secretariat organised an online event to collect **stakeholder's input** to inform and support EDPB's ongoing work on [anonymisation and pseudonymisation](#). This reflects the EDPB's commitment to stakeholder engagement, as outlined in the [Helsinki statement](#).

EDPS-EDPB Joint Opinions

Under Article 42 EUDPR the EDPB and EDPS adopted a joint opinion [01/2025 on the Proposal for a Regulation on simplification measures for Small and Medium Enterprises \(SMEs\) and Small Mid-Cap Enterprises \(SMCs\)](#), in particular the **record-keeping obligation** under Art. 30(5) GDPR. This joint opinion was preceded by a [joint letter on the EC's draft proposal on simplification of record-keeping under the GDPR](#).

Resources management

Human resources

Talent attraction, recruitment and onboarding

In 2025 the EDPS continued to ensure the attraction and recruitment of expertise required for the institution to fulfil its mandate. The focus was set on employer branding, promotion of **diversity**, **selection** and **onboarding** of new staff members as well as interinstitutional cooperation.

During 2025, a total of **19 successful selection procedures** were conducted, resulting in the recruitment of five officials, 13 contract agents and one temporary agent. In addition, a reserve list for contract agents with

AI expertise was established. In response to the new supervisory tasks assigned to the EDPS under the EU AI Act, the EDPS recruited specialised IT profiles to equip the new AI unit with the required technical capacity.

In 2025, the EDPS continued to participate in the inter-institutional **Blue Book Traineeship** programme, offering **two cohorts of ten trainees** the opportunity to join the institution. Given the high interest of EDPS and EDPB teams in this programme and the limited number of traineeship positions available, an internal rotation system was established in 2023 allowing all teams to benefit from it in regular intervals.

In the course of 2025, the EDPS invested in the institution's **employer branding initiative** by ensuring alignment of all HR processes and internal communication across the entire employee lifecycle. Concerning interinstitutional cooperation in the HR field, the EDPS continued to participate in the various working groups and committees.

During 2025, the EDPS started reflections on a new **diversity and inclusion strategy**. For this purpose, the institution participated in various working groups and gathered good practices from other international organisations. To support the strategy formulation, a call for expression of interest for an EDPS internal working group on diversity and inclusion was prepared for launching in 2026.

The **onboarding procedure** for new staff members was improved and administrative steps for the pre-recruitment procedure were simplified. This also involved an increased frequency of onboarding sessions per year and the introduction of a revamped e-welcome package for newcomers.

Talent Retention and HR Enhancements

In 2025, the EDPS implemented key initiatives to enhance workforce stability and staff engagement. In this context, the EDPS adopted a **new talent retention strategy** in 2025 establishing a framework of short, medium and long-term actions designed to retain and develop highly skilled staff. Based on the EU Staff Regulations (SR), the EDPS also initiated preparations for the introduction of new implementing provisions for the recruitment and employment of temporary agents for adoption in 2026.

To improve staff's access to comprehensive and up-to-date information around HR policies and procedures, the HR team launched a series of targeted measures in 2025. These include for example the '**HR Open doors**' initiative and the revamping of the **HR intranet section**. In addition, the EDPS continued to ensure a well-functioning **social dialogue** within the organisation, and facilitated the exchanges between the newly elected staff committee and senior management.

Development of employees, teams and of the organisation

In 2025, the EDPS implemented several actions to foster staff development and institutional growth. In this context, the HR team provided **support** and **guidance** to staff and managers throughout periods of change, such as reorganisations and temporary re-assignments due to absences and turnover.

The EDPS also continued to invest in staff development by promoting **learning** and **development** programmes such as AI training courses, AI and algorithm auditor certifications, customised pleading and public speaking courses and as well as team-building activities.

In addition, a strategy was developed to provide a framework for promoting **wellbeing** at the EDPS. Several cross-unit activities were organised within the scope of this strategy which aimed to enhance staff engagement and cross-team interactions.

Following a call for volunteers launched in late 2024, a thematic cross-unit **working group** of 12 EDPS and EDPB colleagues was established in 2025 to examine the organisation's **energy** consumption, carbon footprint in procurement processes and the commuting means of colleagues. On this basis, the working group plans to promote environmental responsibility through various awareness raising activities in 2026.

Budget

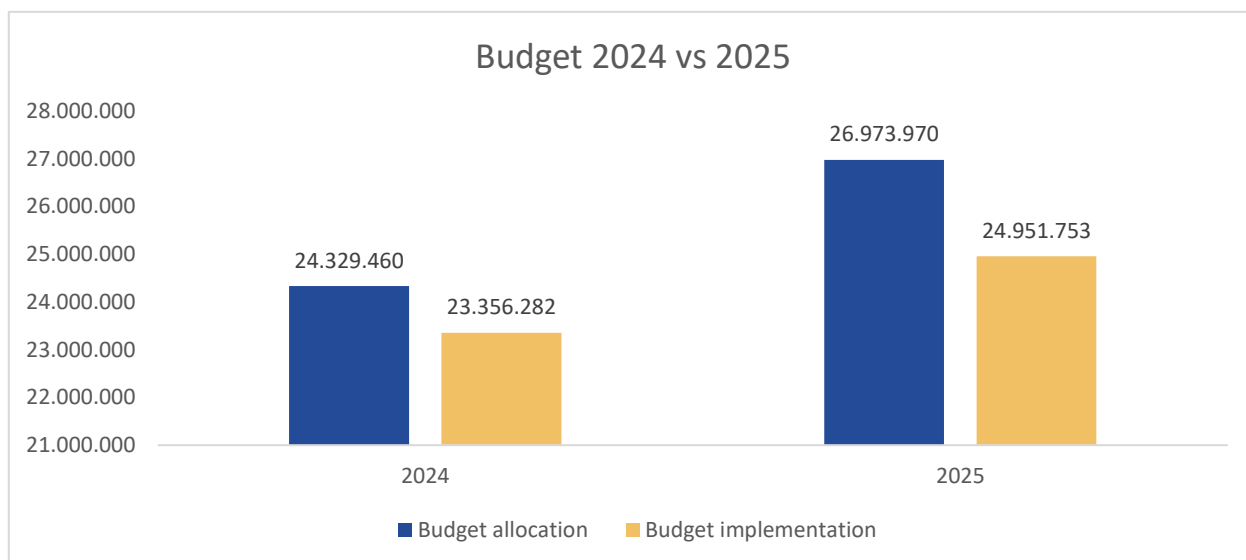
Budget discharge

For the financial year **2023**, the EDPS was **granted discharge**⁷⁴ by the European Parliament. For the financial year **2024**, the discharge procedure is **ongoing**, with results expected in April 2026.

The **European Court of Auditors (ECA)** *did not identify any significant issues* which could give rise to findings concerning the EDPS, as stated in its 2024 annual report⁷⁵. For more details, please see section on ECA. The annual report for the financial year 2025 is expected in Q4 of 2026.

Budget allocation

The EDPS operating budget for 2025 amounted to EUR 26 973 970⁷⁶ marking an **increase of 11%** compared to 2024. This 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.



Budget implementation

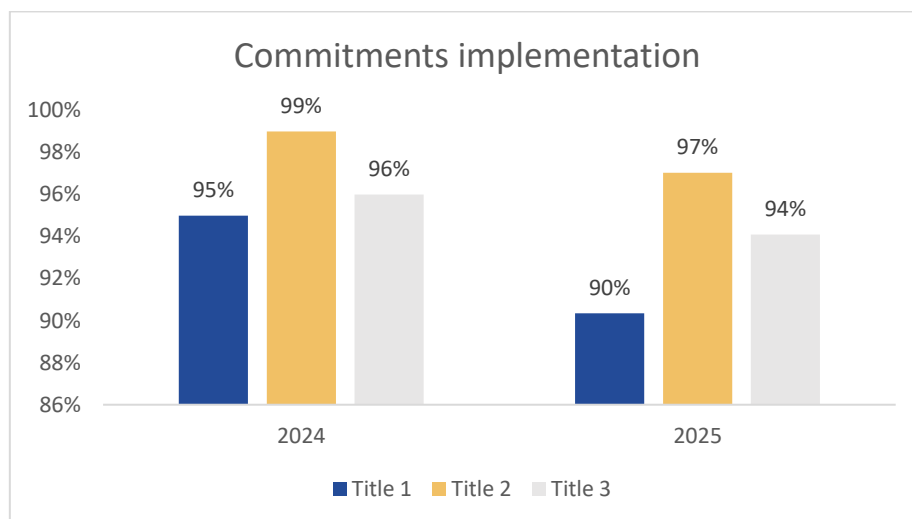
For 2025, the EDPS achieved an overall budget implementation rate of **92,50%**, reflecting rigorous monitoring and sound financial management. More specifically, **staff related costs (Title 1)** reached an implementation rate of **90,35%**. The comparably lower rate was mainly due to a higher-than-anticipated number of vacant posts and unused credits in relation of the delayed nomination of a new Supervisor. Building-related expenditure, **equipment** and other **operational costs (Title 2)** led to an implementation rate of **97,03%**, reflecting effective resource allocation and expenditure monitoring.

⁷⁴ Decision (EU) 2025/1608 of the European Parliament of 7 May 2025 on discharge in respect of the implementation of the general budget of the European Union for the financial year 2023, Section IX – European Data Protection Supervisor https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501608

⁷⁵ ECA annual report 2024: <https://www.eca.europa.eu/en/publications/AR-2024>

⁷⁶ The initial budget of EUR 27 083 875 was amended following a salary update in October 2025 applying to staff of all EU institutions

Expenditure related to the **EDPB (Title 3)** attained an implementation rate of **94,10%**. Budget lines linked to EDPB contractual obligations with other EUIBAs (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.



Detailed figures are available in [Annex 2](#).

Budget for 2026

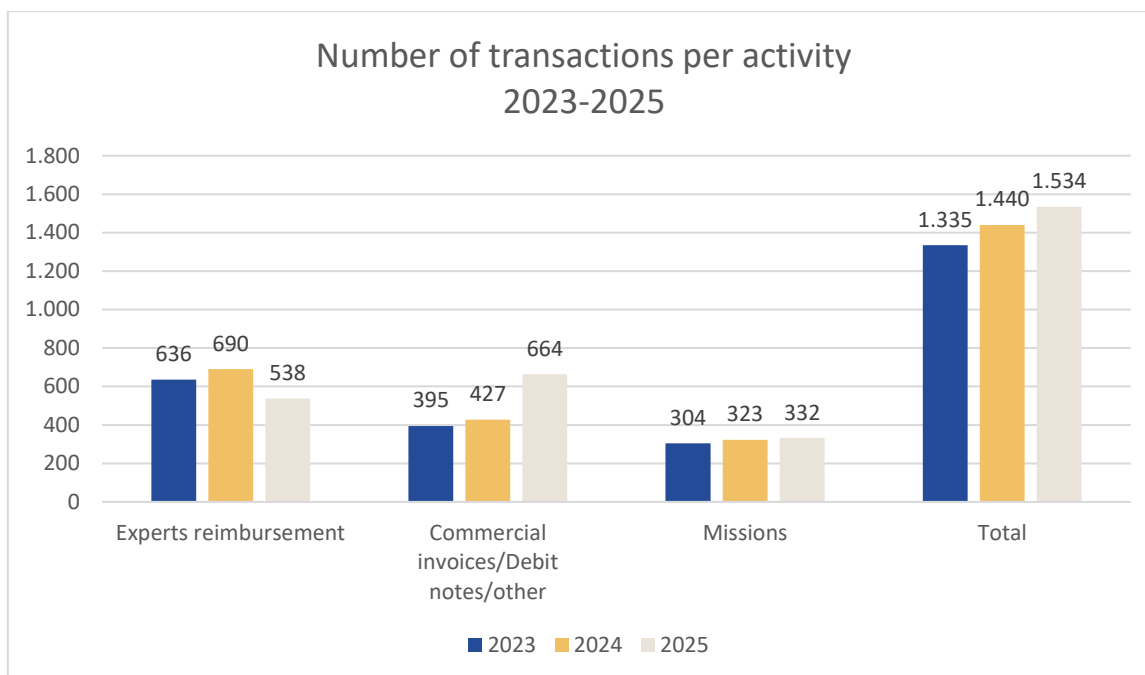
For 2026, the EDPS requested a substantial increase in staff (**+26 posts**) and appropriations (**+27%**). This request was **proportionate** to the growing responsibilities assigned to the institution, in particular under the AI Act and the rapidly evolving digital regulatory framework.

However, as in previous years, strict budgetary discipline regarding administrative expenditure and staffing across EUIBAs influenced the preparation of the 2026 draft budget. Consequently, significant cuts were applied during the budgetary procedure, in line with general savings measures across the whole EU budget. As a result, the Budgetary Authorities could not fully agree with the EDPS' budget request, only granting **12 additional administrative posts** (EU officials), including **five for the EDPB**, as well as **five contract agent** positions. The final approved budget reflects these changes, with a **13,70% increase** in expenditure compared to 2025.

Finance

In 2025, the number of payment transactions reached **1 534**, a slight **increase** of 6,53% compared to 2024 (1 440). For 2025, **99,6%** of payments were processed **on time** (within 30 days). The **average payment time** was **14,62 days**⁷⁷.

⁷⁷ since the EC onboarded SUMMA in 2025 and encountered several initial bugs related to reimbursement claims in AGM during the first five months, related transactions were removed from the 2025 payment time statistics.



Missions, expert payments and salaries are initiated by the **Paymaster Office** of the EC (PMO) in accordance with the Service Level Agreement (SLA) concluded between the respective institutions. These payments are subject to an additional layer of ex-ante controls, which are conducted by the PMO in conjunction with the controls already applied by the EDPS.

Ex-ante controls

In accordance with Article 74(5) of the Financial Regulation, all operations are subject to ex-ante controls. These controls involve the **initiation** and **verification** of an operation prior to its execution, covering both the operational and financial aspects. They are performed by staff with the necessary expertise, appointed by the authorising officer by delegation.

To ensure the effectiveness of these controls, the EDPS uses **checklists** that outline the essential checks to be conducted by the operational and financial agents involved in processing operations. The use of the **Speedwell**⁷⁸ system significantly streamlines the basic controls applied to payments and commitments.

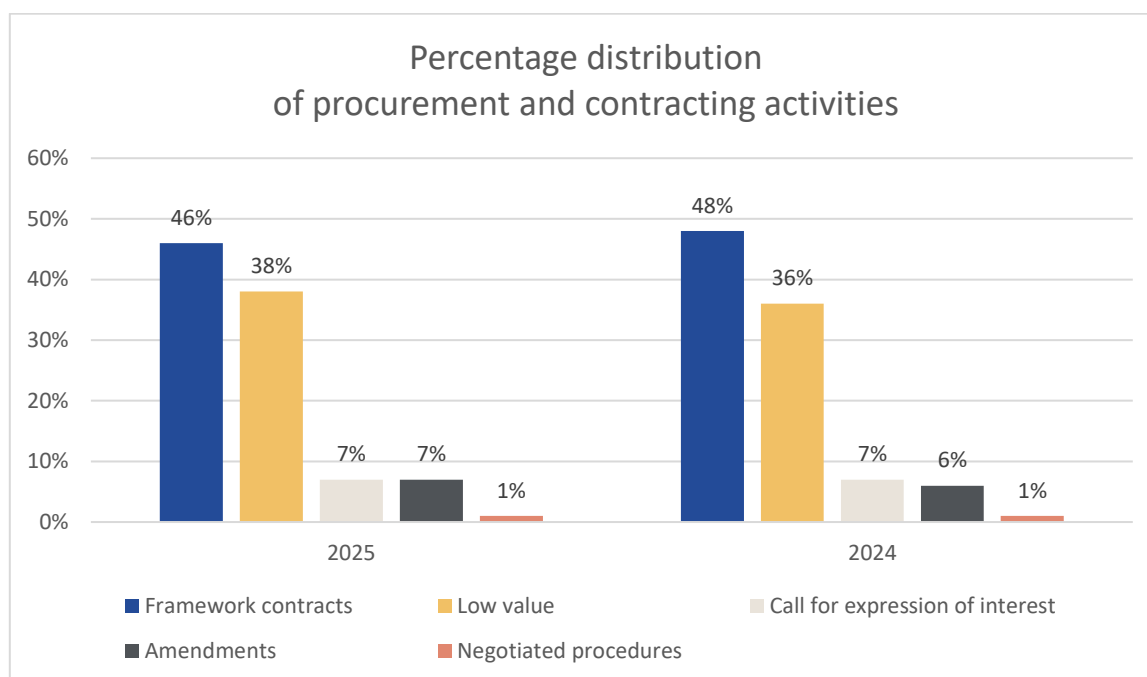
⁷⁸ Since 2020, the EDPS has been using a paperless financial workflow system called Speedwell. This system can be seen as an extension of Accrual Based Accounting System (ABAC), enabling the electronic circulation of invoices among all parties involved in the payment process and guiding them through the verification stage. The system features European Commission Authentication Service (ECAS) access, which ensures the identity of the person granting approval, including the 'certified correct' visa for the invoice and the 'passed for payment'. The implementation of this electronic workflow has ensured business continuity, allowing for a seamless adaptation to new working methods that promote teleworking and enhance both the efficiency of financial transaction processing and the quality of financial and accounting information.

Procurement and contracting

In 2025, the EDPS, acting also on behalf of the EDPB, launched **47** (mostly very low value) **public procurement procedures**, including **one negotiated procedure without prior publication of a contract notice**. Besides, **seven contracts** were awarded to **individual experts** in the context of a call for expression of interest.

In 2025, the EDPS also made use of a significant number of **framework contracts (FWC)** through **46 order forms** and **specific contracts**, including inter-institutional FWC related to IT consultancy, communication activities, interim services and office supplies.

Throughout all procurement procedures, the organisation prioritised an open, fair, transparent selection and competition process, ensuring that external contractors meet high quality standards.



Missions' management

Missions' management at the EDPS is conducted in accordance with the EC applicable rules and internal decisions. In addition, the EDPS has a speaking engagement policy, which clarifies the rules in those cases where the mission expenses should be paid by the organiser and is **selective** as regards **attendance** to external events.

Since November 2022, the EDPS has participated in a PMO project for **shared mission management**, ensuring a centralised and consistent approach to reimbursement requests for missions and related expenses. The PMO verifies supporting documents for compliance with applicable rules, while the EDPS oversees initiation, validation, and related information.

The figures presented in this section stem from the **Missions Tool (MIPS)** and reflect the **consumption** of 2025 commitments concerning the missions of EDPS/EDPB staff, the EDPS Supervisor as well as the EDPB Chair and Deputies. Total costs may require adjustments due to the timing of the billing process.

	2022		2023		2024		2025	
	Supervisor	Staff	Supervisor	Staff	Supervisor	Staff	Supervisor	Staff
Nr. of missions	21	171	24	246	23	218	18	206
Average cost EUR	1488	1035	1 303	999	1 681	853	1 435	758
Total cost EUR	31 267	176 903	31 279	284 580	38 672	185 684	25 829	156 073

Full details on the Supervisor’s missions for 2025 are available in [Annex 3](#).

In addition, in 2025, the EDPB Chair performed 17 missions and her two deputies, five.

Number of missions and cost in 2025		
EDPB Chair		
Chair name	Number of missions	Cost (EUR)
Anu Talus	17	42 236
Irini Loizidou-Nikolaidou/Zdravko Vukic (deputies)	5	6 607

Overall, in 2025, the total cost for the EDPS/EDPB missions amounts to EUR 230 745

IT infrastructure and tools

The **EDPS** acquires its IT infrastructure and tools mainly **through** Memoranda of Understanding (MoUs) and Service Level Agreements (SLAs) with the EP and the EC.

The MoU with the EP covers essential IT infrastructure⁷⁹, while the EC agreements cover hosting data centre and access to Directorate-General for Digital Services’ (DG DIGIT) specific applications⁸⁰ and services. Through these partnerships, the EDPS **maximises synergies** by using tools such as:

- **ARES** (Records Management tool for administrative activities),
- **EU Sign** (qualified signatures),
- **EU Login** (user authentication tool)
- **EU Send** (secure data transmission),
- **ServiceNow** (support tickets management tool)

⁷⁹ Network services, communications, computers, intranet, shared drives, Outlook, video conferencing, and office suites

⁸⁰ ARES, ABAC Assets, AGM, EU Login, EU Send, CIRCABC, EU Survey, EC Framework Contracts, and the web portal

The EDPS also participates in interinstitutional **procurement**. Where partnerships fall short, it develops custom business applications internally.

Systems operated by the EC Directorate-General for Human Resources (DG HR) and for Budget (DG BUDG), namely Sysper 2 and SUMMA, are put at the EDPS disposal for managing **HR**, **budget** and **finance** respectively. In 2025, the EDPS explored **process automation** via DG DIGIT's container orchestration, including a **proof of concept** for data breach notifications.

The EDPS **Case Management System** (CMS), used for documenting core business activities, is using the Fabasoft Folio product⁸¹ tailored to the EDPS' needs with robust data protection safeguards. Its integration into the EDPS' IT environment is supported by the EP. Annual assessments are conducted based on provider documentation and certifications.

The EDPS **Public Key Infrastructure** (PKI) supports secure access to the EDPS CMS. In 2025, the EDPS overcame sourcing and operational delays and completed the redeployment, and started the migration to the new PKI, with enhanced security controls and thorough documentation.

Following a pilot of the **Nextcloud** collaborative platform⁸² with a European cloud service provider, the EDPS decided to discontinue this project due to limited operational and development.

The EDPS also expanded the scope of the information shared via the DG DIGIT service called **Secure European Centralized Address Books & Certificates** (SECABC), to enhance interoperability with other EUIBAs. Finally, the organisation secured early access to DIGIT's '**GPT@EC**' AI and completed the upgrading of the main EDPS videoconferencing room.

Assets' Security & Business Continuity

As an EU institution subject to the Cybersecurity Regulation 2023/2841, the EDPS submitted **four deliverables** in 2025 to fulfil its compliance obligations: (i) an initial cybersecurity review identifying key vulnerabilities; (ii) the initial cybersecurity plan outlining short-term mitigating measures; then the (iii) a cybersecurity maturity assessment based on the CERT-EU methodology; and (iv) a cybersecurity risk assessment incorporating the findings of the preceding deliverables. Together, these form the basis for the EDPS cybersecurity plan submitted to the Inter-institutional Cybersecurity Board (IICB) in accordance with Article 9 of this Regulation.

In parallel, the EDPS implemented targeted **security controls** to strengthen its cybersecurity posture, including the establishment of a cybersecurity framework, training of EDPS and EDPB managers, updates to SLAs and external provider contracts, deployment of technical safeguards, and continuous awareness and training activities.

The management of information security, physical security, business continuity, and the protection of classified information remains essential to safeguarding the EDPS' mission, reputation and business continuity. To support this, the **independent roles** of the Local Information Security Officer (LISO), and the Local Security Officer have been established, both reporting directly to the EDPS Secretary-General, to ensure autonomy.

In 2025, the EDPS maintained and enhanced **key safeguards** for the protection of Sensitive Non-Classified (SNC) information, EU classified information, business continuity, and staff safety, including:

- Revision of the Acceptable Use Policy to reflect technical and organisational changes;
- Regular risk assessments and updates to security plans and information assets;
- A tabletop business continuity exercise simulating a cybersecurity crisis;

⁸¹ Supplied by Fabasoft to the EDPS, as Software as a Service (SaaS), under the SIDE III Framework Contract

⁸² The package the EDPS negotiated for "Nextcloud with optional Collabora Office" was included in the list of group S (SaaS) negotiated packages under the SIDE II Framework Contract, so that other EUIBAs could easily procure Nextcloud hosted services.

- Implementation of an emergency notification system for staff safety and business continuity;
- Improvements of internal safety mechanisms following lessons learned from security incidents;
- Management of Restricted lapTOPs for staff handling EU classified information;
- Continuous staff awareness and training on safety and business continuity.

Internal control

Control results

Effectiveness

a. Legality and regularity of transactions

The EDPS uses internal control processes to ensure sound management of risks relating to the legality and regularity of the underlying transactions it is responsible for.

The control objective is to ensure that the EDPS has reasonable assurance that the total amount of any financial operation authorised during the reporting year, which would not be in conformity with the applicable contractual or regulatory provisions, **does not exceed 2% of the authorised payments concerned**, a threshold used also by the European Court of Auditors (ECA). To reach this conclusion, the EDPS reviewed the results of the key controls in place (as described below). For each item, materiality is assessed in accordance with the materiality criteria as adopted by the ECA.

Objectives of materiality criteria:

The materiality threshold gives the AOD a basis on which to establish the significant weaknesses that require a formal reservation to his statement. The assessment of a weakness falls to the qualitative and quantitative judgment of the AOD, who remains responsible for the statement of assurance, including the reservations made.

Qualitative and quantitative criteria for determining the level of materiality:

a) Qualitative criteria

The following parameters were used to establish significant weaknesses:

- significant/repeated errors without mitigation;
- weakness in the internal control system;
- insufficient supporting documents;
- material problems identified by the ECA and/or the IAS;
- problems of reputation.

b) Quantitative criteria

Once a significant weakness has been identified, quantitative criteria must be applied to determine the level of materiality. This level will be used to determine whether the weakness 'merits' being reported.

- margin of error
- maximum amount of risk.

Should the residual risk of an error be higher, the institution must explain the reasons for it. The EDPS materiality threshold (2% of annual appropriations) is: EUR 539 479,4 (2% of the 2025 budget after transfers)

b. Ethics

The EDPS prioritises professional ethics, promoting excellence in the European civil service and safeguarding the framework of rights and obligations outlined in the SR. To guide staff conduct, the EDPS has established an ethics framework, comprising a **Code of conduct** for the **Supervisor**⁸³ and a separate **Code of conduct** for all **staff**, as well as decisions on **whistleblowing, anti-harassment, disciplinary proceedings** and **administrative investigations**.

In line with the specific Code of conduct for the Supervisor, the latter completed and published his **annual declaration of interest** for 2025⁸⁴.

New staff attend a mandatory **presentation** on the ethics framework and on anti-harassment policy during onboarding. In 2025, **three** onboarding sessions were held for 34 newcomers.

During 2025, the EDPS Ethics officer, staff member in charge of coordinating activities related to ethics, advised staff on ethical matters and received **41 formal requests** (against 30 in 2024) related to the Code of Conduct for staff. Most requests concerned the authorisation for carrying out external activities (in particular lectures, presentations and patronage) and publications. The e-workflow for ethics requests - added to Sysper in 2023 - was successfully tested for EDPB staff members in 2024. A full deployment for all staff was achieved in the course of 2025.

During the reporting year, the Investigation and Disciplinary Office of the European Commission (**IDOC**) closed an administrative inquiry which was initiated in 2024 on behalf of the EDPS, into an alleged case of ethical misconduct with the recommendation made to the EDPS to initiate disciplinary proceedings in accordance with the SR. In addition, the EDPS was involved in **three** investigations of the European Anti-Fraud Office (**OLAF**) which are ongoing.

The European Ombudsman following **five complaints** against the EDPS, initiated **three inquiries**⁸⁵. Two of them concerned the alleged failure to take a timely decision and one the alleged failure to deal properly with requests for information (3121/2025/IJ). All of them have been resolved and **closed with no findings of maladministration**.

Finally, pursuant to the new EDPS decision on transparency measures, the Supervisor, the Head of the EDPS Secretariat, and EDPS managers will engage exclusively with interest representatives registered in the **Transparency Register**⁸⁶. This provision ensures that interest representatives are registered in the interinstitutional transparency register, and that interactions are publicly disclosed, thereby enhancing institutional accountability.

c. Deviations' reporting

All deviations are signed by the authorising officer in charge. In 2025, **16 events** were recorded: 14 derogations⁸⁷, one non-compliance event⁸⁸ and one prior approval. Compared to 2024 (14 events), the overall number of deviations **increased**.

⁸³ https://www.edps.europa.eu/sites/default/files/publication/2019-12-06_code_of_conduct_supervisor_en.pdf

⁸⁴ Declaration of interests of the Supervisor, 24 January 2025 https://www.edps.europa.eu/system/files/2025-01/declaration_of_interest_wiewiorowski_2025_final_en.pdf

⁸⁵ 1) [3047/2025/ET](https://www.edps.europa.eu/system/files/2025-01/3047/2025/ET), 2) [3121/2025/IJ](https://www.edps.europa.eu/system/files/2025-01/3121/2025/IJ), 3) [3531/2025/ET](https://www.edps.europa.eu/system/files/2025-01/3531/2025/ET)

⁸⁶ The transparency register https://transparency-register.europa.eu/index_en

⁸⁷ Derogations are explicit situations allowed or foreseen in the processes and procedures under specific circumstances.

⁸⁸ A non-compliance event is a deviation from established processes and procedures or gaps in existing controls, detected only **after** the expense occurred (ex post).

d. Accounting controls

The **EC's accountant** also serves as the accounting officer of the EDPS. Inter-institutional cooperation offers numerous benefits from a financial management and budget consolidation perspective. For the EDPS, this **cooperation** is essential due to its limited size and resources, as it enables efficiency gains and economies of scale. Moreover, since most expenditures are incurred within EU administrations, this cooperation yields significant savings for the EU budget. This collaborative approach is formalised through SLAs.

The EDPS has established **robust procedures** and **controls** to ensure the accuracy, completeness and timeliness of accounting data and related information used to prepare its annual accounts and financial reports. One full-time-equivalent (FTE) was recruited to serve as an **accounting correspondent**.

e. Ex-post controls

According to Article 74(6) of the Financial Regulation, the authorising officer can organise, in addition to the mandatory ex-ante controls, also ex-post controls on sample basis depending on risks related to the transactions.

In 2025, ex-post controls were conducted on missions' management following a risk assessment. While **no financial errors were identified**, weaknesses in the legal framework and its implementation were observed, impacting the legality and regularity of related transactions. A revision is underway to address these shortcomings.

Since the selected methodology for running the exercise was risk-based, the sample cannot be considered representative and therefore the results cannot be extrapolated to all payments.

Efficiency

During 2025, **99,60%** of payments were processed **on time** (within 30 days). In addition, **92,50%** of the budget was **executed** against a target of 90%, as set in the [key performance indicator nr. 9](#). For carrying out a cost-benefit analysis, the EDPS, being a small Institution, takes as a base the model applied by the EPSO, since as the EDPS, it **only manages administrative appropriations** under Heading V of the EU budget. This model consists of a single global indicator which is calculated by dividing the approximate total cost of control by all expenditure made during the year (budget implementation in terms of payments).

The total number of FTEs involved in the main control activities (internal control, procurement and finance) is estimated at around eight FTEs. The estimated average cost (all categories of cost included) of the control activities for 2025 amounts to **EUR 737 931**. The total budget implementation in terms of payments for 2024 is EUR 22 537 804. This means that the cost of the control activities **dropped to 3,27%** of the EDPS expenditure in comparison to last year (3,96% of EUR 20 712 599). The more than 20% decrease in control activities' costs is explained by an increase in underlying payments and the replacement of one administrator-level official with an assistant-level official within the eight FTEs involved in these activities.

Consequently, based on an assessment of the most relevant key indicators and control results, the EDPS has assessed the efficiency of the control system and reached a positive conclusion.

Audit observations

In 2025, the Internal Audit Service (IAS) completed one audit, closed one recommendation from a past audit and carried out a risk assessment exercise for establishing the 3-year audit plan for the EDPS. IAS did not

identify any critical or very important⁸⁹ recommendation. The ECA completed its Statement of Assurance (SoA) for the 2024 financial year, and the preliminary part of the 2025 SoA; none of the two exercises gave rise to any findings. Details follow in dedicated sections below.

Internal Audit Service

In June 2025, the IAS completed the audit of 'governance arrangements for information technology (IT) services provided by the EP to the EDPS', which concluded that the EDPS has *adequately designed and effectively and efficiently implemented governance arrangements for the IT services provided by the EP*, while detecting points for improvement. Two important recommendations were formulated: one concerning the Service Level Agreement (SLA) between the two parties, and another addressing the governance and process management framework for the IT services provided.

For addressing these recommendations, the EDPS will focus on updating the SLA with the EP to reflect new legislative requirements and to strengthen its implementation and monitoring. In addition, further actions aim to clarify the roles and responsibilities of both parties, as well as to define clear mechanisms for conflict resolution, should the need arise.

The corresponding EDPS action plan was approved by IAS and is currently under implementation.

Regarding previous audit recommendations, the implementation of one very important recommendation remains pending. It stems from the 2023 audit on the 'methodology for the planning of the EDPS audits in the EDPS'. In 2025, most related actions were implemented. The methodology was updated to clarify roles and responsibilities, the "audit universe" is now clearly defined, and a risk-based approach has been introduced to prioritise audits. Improvements were also made to the process for estimating the human resources required to implement the audit plan. However, the establishment of a long-term EDPS strategy remains pending, as this falls under the prerogative of the new Supervisor to be appointed. Its implementation has therefore been postponed until the end of April 2026.

Finally, the important recommendation stemming from the same audit, on the implementation of the EDPS audit plan, was completed and closed by IAS as adequately and effectively implemented.

European Court of Auditors

In October 2025, the ECA published its 2024 Annual Report⁹⁰, in which the EDPS features in Chapter 10, "European public administration". In 2024, as every year, the ECA carried out its Statement of Assurance (SoA) exercise, which included one sample relating to salaries, as well as an audit of the budgetary reports. Neither exercise identified any significant issues that could give rise to a finding.

The SoA exercise for the financial year 2025 was initiated in Q4 2025 and is scheduled to be finalised in July 2026. The preliminary results, referring to the examination of procuring a service through the use of an EC framework contract, did not give rise to any findings.

Annual planning and risk management

The objectives are defined in the Strategy⁹¹ and reflected in the Annual Management Plan (AMP) in the form of concrete actions and deliverables throughout the coming year. The AMP plan translates the EDPS long-

⁸⁹ The IAS characterisation of recommendations is the following: 'critical', 'very important', 'important'.

⁹⁰ 2024 Annual Report of the European Court of Auditors : <https://www.eca.europa.eu/en/publications/AR-2024>

⁹¹ https://www.edps.europa.eu/sites/default/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf

term strategy into general and specific objectives. Three times per year, a review is carried out for monitoring the progress in meeting the targets as set in the AMP.

The AMP also includes KPIs, defined in the Strategy 2020-2024, which are regularly measured for monitoring the progress achieved during the implementation phase. See [here](#) more information on KPIs for 2025.

An annual risk assessment exercise is performed in parallel with the AMP for instilling risk culture when planning activities. A structured follow-up is performed six months after the adoption of annual results, ensuring effective oversight of risks.

Internal control annual assessment

Based on the EDPS decision of 06 October 2020 on the adoption of the Internal Control Standards (ICS), their assessment is done through examination of 14 standards, grouped up in six building blocks:

- I. Mission and values (1. Mission, 2. Ethical and organisational values)
- II. Human Resources (3. Staff Allocation and Mobility 4. Staff Evaluation and Development)
- III. Planning and Risk Management Processes (5. Objectives and Performance Indicators, 6. Risk Management Process)
- IV. Operations and Control Activities (7. Operational Structure, 8. Processes and Procedures, 9. Management Supervision, 10. Business Continuity, 11. Document Management)
- V. Information and Financial Reporting (12. Information and Communication, 13. Accounting and Financial Reporting)
- VI. Evaluation and Audit (ICS14)

The 2025 ICS assessment confirmed a satisfactory overall level of internal control, with all six building blocks present and functioning. The effectiveness of building blocks I, II, IV, and VI could be improved, particularly in ICS 2, ICS 3, ICS 4, ICS 7, ICS 8, ICS 10, ICS 11 and ICS 14.

Space for improvements was identified in strengthening governance frameworks, enhancing organisational resilience, and ensuring greater consistency in internal processes. Priorities include reinforcing oversight and monitoring mechanisms, addressing structural and resource-related challenges, and advancing the implementation of outstanding actions and recommendations.

Conclusions on the assurance

This section reviews the assessment of the elements reported above (in Sections 4.1-4.4), and the sub-conclusions already reached. It draws an overall conclusion to support the declaration of assurance and whether it should be qualified with reservations.

The assessment of the elements and the conclusions reported in these sections result from a systematic analysis of the evidence available. The following elements provide sufficient guarantees as to the completeness and reliability of the information reported and results in a comprehensive coverage of the budget delegated to the Secretary-General of the EDPS:

- the EDPS has put in place suitable ethic mechanisms to limit risks of error and prevent, detect and correct fraud and irregularities,
- the EDPS' internal controls systems provide sufficient assurance to adequately manage the risks relating to the legality and regularity of the underlying transactions,
- the EDPS implemented appropriate ex-ante and ex-post controls, to the extent that they remain cost-effective,
- recommendations issued by the EDPS' auditing bodies do not raise any assurance implications and are being implemented as part of the ongoing continuous efforts in terms of further improvements,

- the EDPS' internal control system allows for proper planning of activities, detecting areas for improvement and ensures through appropriate mechanisms an efficient follow-up and correction where appropriate with regards to the achievement of the internal control objectives,
- resources were used for the intended purposes and non-omission of significant information was ensured.
- the hand-over report of the staff member who served as an AOD from September 2025 until end of February 2026 did not give rise to any significant management issue.

In conclusion, based on the elements reported above, management has reasonable assurance that, overall, suitable controls are in place and working as intended; risks are being appropriately identified, monitored and mitigated and necessary improvements and reinforcements are being implemented. The EDPS Secretary-General, in his capacity as authorising officer by delegation has signed the declaration of assurance.

Declaration of assurance

I, the undersigned, Leonardo CERVERA NAVAS, EDPS Secretary-General, in my capacity as authorising officer by delegation

Declare that the information contained in this report presents a true and fair view.

State that, I have had reasonable assurance that the resources allocated to the activities described in this report have been used for the intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying operations.

This reasonable assurance is based on my own judgment and on the information available to me, such as the results of the self-evaluation, ex-post controls and the report of the Internal Audit Service.

Confirm that I am not aware of any matter not reported in the present report which could harm the interests of the institution.

e-signed

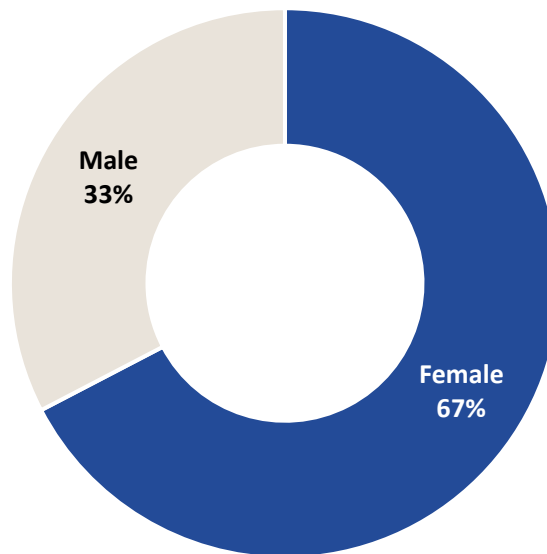
in Brussels

Annexes

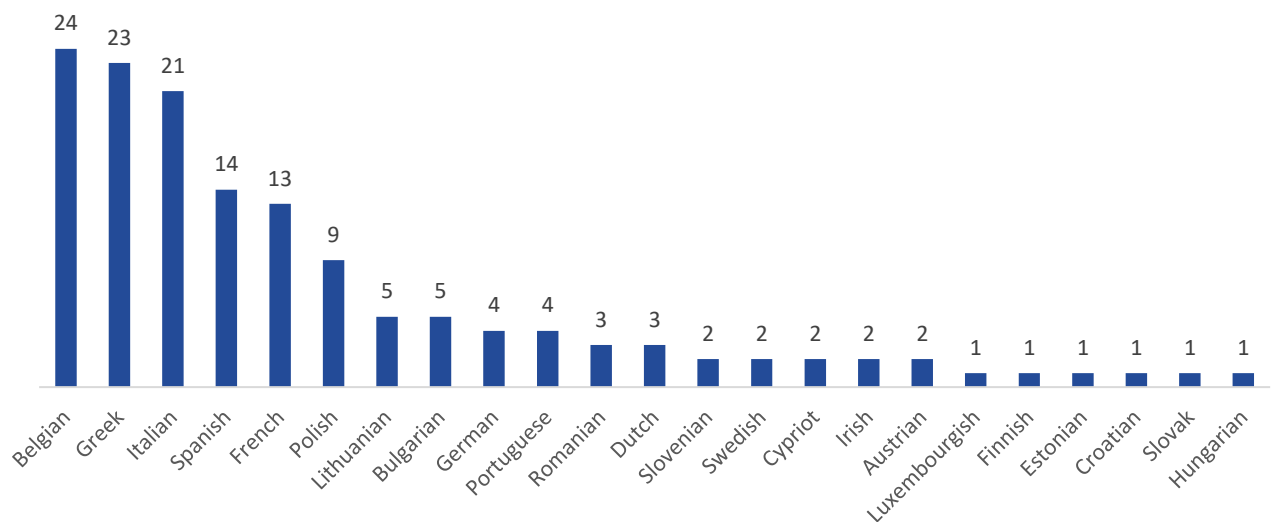
Human resources at the EDPS/EDPB

The charts below provide a snapshot of the situation on 31 December 2025.

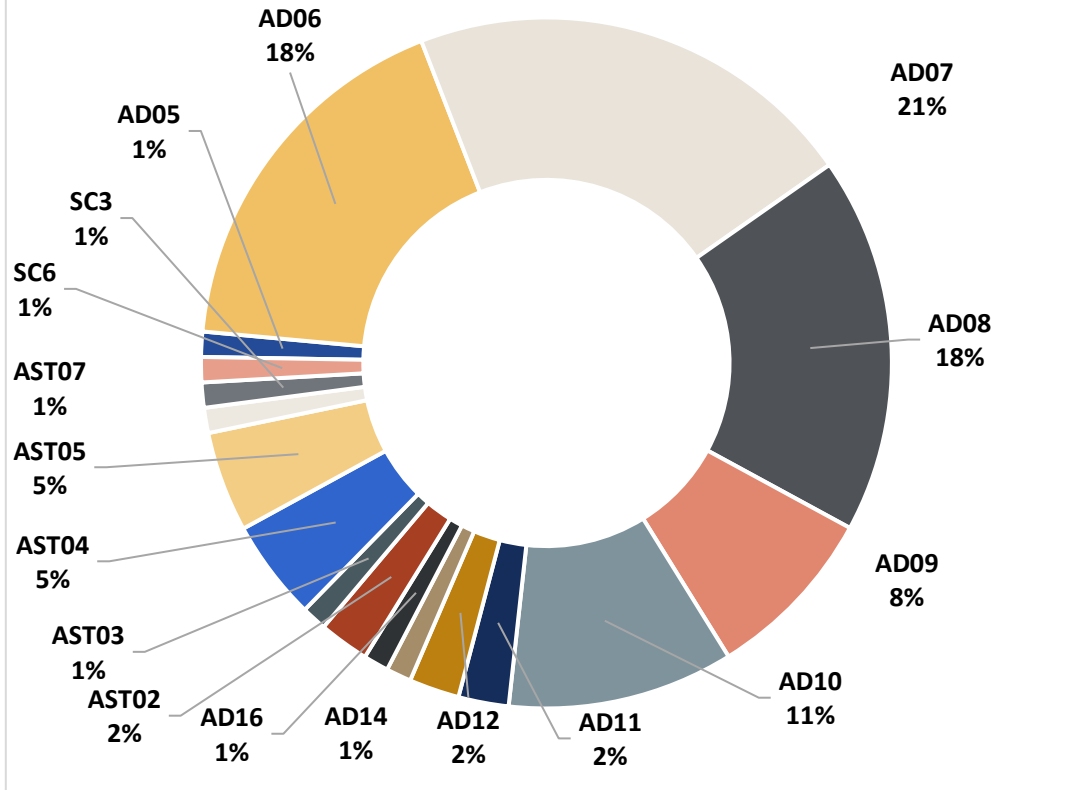
Active statutory staff members per gender at EDPS/EDPB



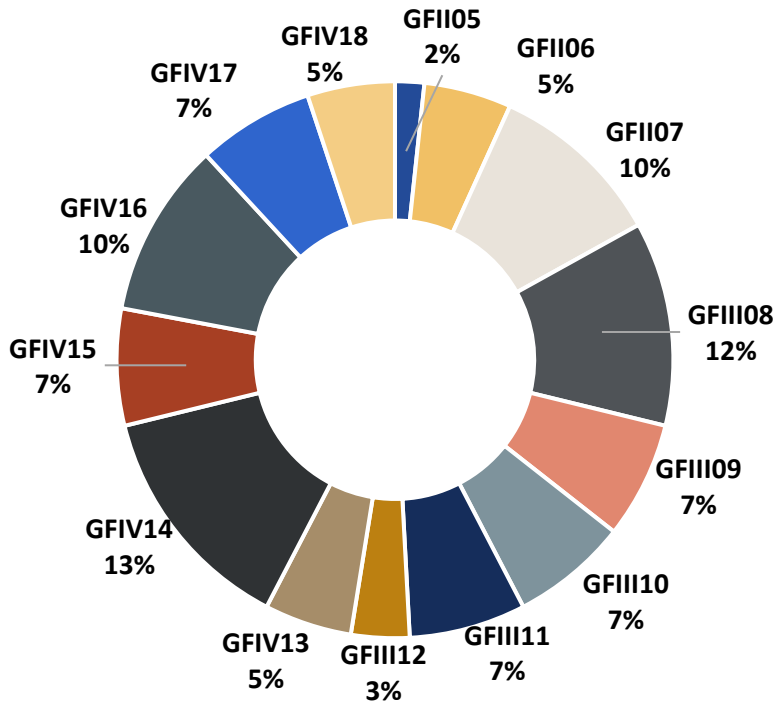
Active statutory staff members per nationality at EDPS/EDPB



Officials and Temporary Agents



Contract Agents per grade



Budget in 2025

TITLE 1 - EXPENDITURE RELATING TO PERSONS WORKING WITH THE INSTITUTION		2024 (after transfers)	Execution 2024	2025 (after transfers)	2025 vs 2024	2025 vs 2024 (%)	execution 2025 (%)
Chapter 10	Members of the institution						
Article 100	Remuneration, allowances and other entitlements of Members						
	Item 1000 Remuneration and allowances	436.000,00	97,61%	457.000,00	21.000,00	4,82%	99,55%
	Item 1001 Entitlements on entering and leaving the service	2.650,00	99,89%	74.687,00	72.037,00	2718,38%	100,00%
	Item 1002 Temporary allowances	0,00		169.984,00	169.984,00		0,00%
	Item 1003 Pensions	0,00		0,00	0,00		
	Item 1004 Provisional appropriation	0,00		0,00	0,00		
	TOTAL Article 100	438.650,00	97,62%	701.671,00	263.021,00	59,96%	75,48%
Article 101	Other expenditure in connection with Members						
	Item 1010 Further training	0,00	0,00%	5.000,00	5.000,00		0,00%
	Item 1011 Mission expenses, travel expenses and other ancillary expenditure	43.000,00	100,00%	40.000,00	-3.000,00	-6,98%	100,00%
	TOTAL Article 101	43.000,00	100,00%	45.000,00	2.000,00	4,65%	88,89%
	TOTAL Chapter 10	481.650,00	97,84%	746.671,00	265.021,00	55,02%	76,29%
Chapter 11	Staff of the institution						
Article 110	Remuneration, allowances and other entitlements of officials and temporary staff						
	Item 1100 Remuneration and allowances	8.713.350,00	95,74%	10.099.593,00	1.386.243,00	15,91%	91,35%
	Item 1101 Entitlements on entering, leaving the service and on transfer	85.000,00	50,55%	90.000,00	5.000,00	5,88%	77,62%
	Item 1102 Overtime	0,00		0,00	0,00		
	Item 1103 Special assistance grants	0,00		0,00	0,00		
	Item 1104 Allowances and miscellaneous contributions in connection with early termination of service	0,00		0,00	0,00		
	Item 1105 Provisional appropriation	0,00		0,00	0,00		
	TOTAL Article 110	8.798.350,00	95,30%	10.189.593,00	1.391.243,00	15,81%	90,16%
Article 111	Other staff						
	Item 1110 Contract staff	2.247.594,00	97,51%	2.707.466,00	459.872,00	20,46%	99,18%
	Item 1111 Cost of traineeships and staff exchanges	245.000,00	84,06%	340.000,00	95.000,00	38,78%	59,53%
	Item 1112 Services and work to be contracted out	60.000,00	90,92%	63.000,00	3.000,00	5,00%	100,00%
	TOTAL Article 111	2.552.594,00	96,07%	3.110.466,00	557.872,00	21,86%	94,87%
Article 112	Other expenditure in connection with staff						
	Item 1120 Mission expenses, travel expenses and other ancillary expenditure	150.000,00	100,00%	153.000,00	3.000,00	2,00%	100,00%
	Item 1121 Recruitment costs	10.000,00	50,00%	14.000,00	4.000,00	40,00%	6,31%
	Item 1122 Further training	89.000,00	60,59%	90.780,00	1.780,00	2,00%	56,00%
	Item 1123 Social service	0,00		35.461,00	35.461,00		1000,00%
	Item 1124 Medical service	30.000,00	64,48%	30.000,00	0,00	0,00%	100,00%
	Item 1125 Union nursery centre and other day nurseries and after-school centres	100.000,00	79,28%	82.000,00	-18.000,00	-18,00%	100,00%
	Item 1126 Relations between staff and other welfare expenditure	21.000,00	57,00%	17.539,00	-3.461,00	-16,48%	76,38%
	TOTAL Article 112	400.000,00	79,88%	422.780,00	22.780,00	5,70%	86,47%
	TOTAL Chapter 11	11.750.944,00	94,94%	13.722.839,00	1.971.895,00	16,78%	91,11%
	TOTAL TITLE 1	12.232.594,00	95,06%	14.469.510,00	2.236.916,00	18,29%	90,35%

TITLE 2 - BUILDINGS, EQUIPMENT AND EXPENDITURE IN CONNECTION WITH THE OPERATION OF THE INSTITUTION		2024 (after transfers)	Execution 2024	2025 (after transfers)	2025 vs 2024	2025 vs 2024 (%)	execution 2025 (%)
Chapter 20	Buildings, equipment and expenditure in connection with the operation of the institution						
Article 200	Rents, charges and buildings expenditure	1.751.494,00	100,00%	1.855.972,00	104.478,00	5,97%	100,00%
	TOTAL Article 200	1.751.494,00	100,00%	1.855.972,00	104.478,00	5,97%	100,00%
Article 201	Expenditure in connection with the operation and activities of the institution						
	Item 2010 Information technology equipment and services	911.620,00	99,21%	1.088.608,00	176.988,00	19,41%	97,29%
	Item 2011 Furnitures, office supplies and telecommunication costs	12.000,00	100,00%	15.000,00	3.000,00	25,00%	60,05%
	Item 2012 Other operating expenditure	458.884,00	98,40%	556.330,00	97.446,00	21,24%	97,08%
	Item 2013 Translation and interpretation costs	190.000,00	100,00%	108.200,00	-81.800,00	-43,05%	80,85%
	Item 2014 Expenditure on publishing and information	140.888,14	98,42%	87.200,00	-53.688,14	-38,11%	87,58%
	Item 2015 Expenditure in connection with the activities of the institution	225.227,86	96,81%	88.000,00	-137.227,86	-60,93%	83,69%
	Item 2016 Experts reimbursements	45.000,00	78,88%	30.000,00	-15.000,00	-33,33%	46,67%
	TOTAL Article 201	1.983.620,00	98,12%	1.973.338,00	-10.282,00	-0,52%	93,67%
	TOTAL CHAPTER 20	3.735.114,00	99,00%	3.829.310,00	94.196,00	2,52%	97,03%
	TOTAL TITLE 2	3.735.114,00	99,00%	3.829.310,00	94.196,00	2,52%	97,03%

TITLE 3 - EUROPEAN DATA PROTECTION BOARD (EDPB)		2024 (after transfers)	Execution 2024	2025 (after transfers)	2025 vs 2024	2025 vs 2024 (%)	execution 2025 (%)
Article 300	Rents, charges and buildings expenditure						
	Item 3000 Rents, charges and buildings expenditure	704.223,40	100,00%	663.000,00	-41.223,40		100,00%
	TOTAL Article 300	704.223,40	100,00%	663.000,00	-41.223,40		100,00%
Article 301	Remuneration, allowances and other entitlements of officials and temporary staff						
	Item 3010 Remuneration and allowances	2.411.500,00	94,56%	2.525.184,00	113.684,00	4,71%	93,24%
	Item 3011 Entitlements on entering, leaving the service and on transfer	30.000,00	82,80%	20.000,00	-10.000,00	-33,33%	0,00%
	Item 3012 Allowances and miscellaneous contributions in connection with early termination of service						
	TOTAL Article 301	2.441.500,00	94,41%	2.545.184,00	103.684,00	4,25%	93,24%
Article 302	Other staff						
	Item 3020 Contract staff	1.734.152,00	98,40%	1.778.752,00	44.600,00	2,57%	94,65%
	Item 3021 Cost of traineeships and staff exchanges	37.000,00	100,00%	115.000,00	78.000,00	210,81%	24,10%
	Item 3022 Services and work to be contracted out	60.000,00	99,02%	95.330,00	35.330,00	0,00%	100,00%
	TOTAL Article 302	1.831.152,00	98,45%	1.989.082,00	157.930,00	8,62%	90,83%
Article 303	Other expenditure in connection with staff of the Board						
	Item 3030 Mission expenses, travel expenses and other ancillary expenditure	57.500,00	100,00%	49.000,00	-8.500,00	-14,78%	100,00%
	Item 3031 Recruitment costs	3.000,00	100,00%	5.410,00	2.410,00	80,33%	0,00%
	Item 3032 Further training	36.000,00	67,48%	41.920,00	5.920,00	16,44%	48,13%
	Item 3033 Medical service	15.000,00	59,08%	17.000,00	2.000,00	13,33%	88,24%
	Item 3034 Union nursery centre and other day nurseries and after-school centres	35.000,00	93,00%	45.000,00	10.000,00	28,57%	88,89%
	TOTAL Article 303	146.500,00	86,15%	158.330,00	11.830,00	8,08%	78,43%
Article 304	Expenditure in connection with the operation and activities of the Board						
	Item 3040 EDPB plenaries and sub-group meetings	307.051,60	92,93%	304.500,00	-2.551,60	-0,83%	99,21%
	Item 3041 Translation and interpretation costs	800.108,00	93,31%	604.500,00	-195.608,00	-24,45%	99,91%
	Item 3042 Expenditure on publishing and information	126.400,00	90,09%	122.300,00	-4.100,00	-3,24%	70,38%
	Item 3043 Information technology equipment and services	1.281.617,00	99,41%	1.492.700,00	211.083,00	16,47%	98,88%
	Item 3044 Furnitures, office supplies and telecommunication costs	12.000,00	15,14%	26.000,00	14.000,00	116,67%	19,03%
	Item 3045 External consultancy and studies	312.000,00	99,86%	252.020,00	-59.980,00	-19,22%	97,90%
	Item 3046 Other expenditure in connection with the activities of the EDPB	196.700,00	80,10%	194.514,00	-2.186,00	-1,11%	82,94%
	Item 3047 Other operating expenditure	152.500,00	99,71%	271.020,00	118.520,00		97,19%
	Item 3048 EDPB Chair and Vice chairs expenses	50.000,00	100,00%	52.000,00	2.000,00		100,00%
	TOTAL Article 304	3.238.376,60	95,65%	3.319.554,00	81.177,40	2,51%	95,80%
	TOTAL CHAPTER 30	8.361.752,00	96,10%	8.675.150,00	313.398,00	3,75%	94,10%
	TOTAL TITLE 3	8.361.752,00	96,10%	8.675.150,00	313.398,00	3,75%	94,10%
	TOTAL BUDGET	24.329.460,00	98,23%	26.973.970,00	2.644.510,00	10,87%	92,50%

List of missions undertaken by the Supervisor in 2025

Missions undertaken by the Supervisor in 2025				
Wojciech Rafał Wiewiórowski				
	Date from	Date to	Purpose	Cost (EUR)
1.	23/02/2025	26/02/2025	16th Meeting of the Joint Parliamentary Scrutiny Group {JPSG) on the European Union Agency for Law Enforcement Cooperation {Europol), Warsaw, (POL)	1 180,35
2.	11/03/2025	12/03/2025	Speaker invitation in the ICRC Workshop, Cambridge, 10-12 March 2025, Cambridge (GBR)	172,45
3.	13/03/2025	15/03/2025	ROME Meeting on the State of Artificial Intelligence Regulations, Policies, and Upcoming Challenges, Rome (ITA)	1 038,90
4.	03/04/2025	03/04/2025	Speaker invitation in Cyber Forum 3 april 2025, Lille (FRA)	166,89
5.	12/05/2025	14/05/2025	Participation in the Privacy Symposium 2025, Venice, 12-16 May 2025, Venice (ITA)	1 919,45
6.	15/06/2025	23/06/2025	Canada Japan- OECD Expert workshop and High-level Roundtable -Participation in the G7 Data Protection and Privacy Authorities I11 Ottawa, 17-20 June 2025; 2025 POC Privacy Symposium, Ottawa (CAN)	284,45
7.	30/06/2025	03/07/2025	EDPB High-level meeting Helsinki (FIN)	1 514,36
8.	04/09/2025	04/09/2025	Keynote at the ECPC Advanced Master's in Privacy, Cybersecurity, and Data Management, Maastricht (NDL)	71,93
9.	13/09/2025	20/09/2025	Global Privacy Assembly (GPA) 2025 - Seoul, 15-19 September 2025, Seoul (KOR)	3 475,96
10.	13/09/2025	24/09/2025	Global Privacy Assembly (GPA) 2025 - Seoul, 15-19 September 2025 International event in Tokyo to discuss current trends on protection and	8 115,59

			utilization of personal data, by having heads of Data Protection Authorities, Seoul (KOR), Tokyo (JPN)	
11.	25/09/2025	26/09/2025	International Organisations Workshop 2025 in Paris (FRA)	657,18
12.	08/10/2025	09/10/2025	World AI Summit Agenda - AMSTERDAM MIF 2025 – AI, CYBERSECURITY, QUANTUM FORESIGHT Building Trust in an Era of Technological Disruption - Paris (FRA), Amsterdam (NDL)	748,06
13.	20/10/2025	22/10/2025	CIPL Europe Summit Amsterdam; IPEN Event in Frankfurt; AFP Event in Frankfurt (DEU)	1 379,85
14.	24/11/2025	25/11/2025	17th Scientific Conference Internet Security – Cyber-responsibility, which will take place on November 24–26, 2025, in Warsaw (POL)	691,08
15.	27/11/2025	29/11/2025	57th EDPS-DPO meeting - 26-28 November 2025 - EFSA, Parma (ITA)	888,36
16.	09/12/2025	10/12/2025	Warsaw Conference, panel: Key aspects of personal data protection in light of the AI Framework Convention), Warsaw (POL)	733,82
17.	03/02/2026*	06/02/2026	Invitation-18th Meeting of the JPSG on Europol, 4-5 February 2026, Nicosia (CYP)	1 534,14
18.	09/03/2026*	11/03/2026	2026 Missions to Strasbourg Office, (FRA)	1 255,77
Total:				25 828,60

* PREC Missions - Missions under 2025 budget taking place in Q1 2026