



# EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data  
protection authority

***"2024 Annual Activity Report"***



# Contents

<b>Abbreviations.....</b>	<b>4</b>
<b>Introduction.....</b>	<b>7</b>
EDPS Highlights of the year.....	7
Strategy .....	8
Key performance indicators.....	8
<b>Operational achievements .....</b>	<b>10</b>
<b>European Data Protection Supervisor .....</b>	<b>10</b>
Supervisory tasks .....	10
Advisory tasks .....	22
Advocacy and Cooperation.....	24
Technology monitoring tasks.....	30
Data Protection Activities.....	32
Access to documents .....	33
Communication.....	33
Creation of the Artificial Intelligence Unit .....	34
<b>Secretariat of the European Data Protection Board .....</b>	<b>35</b>
Analytical support to EDPB activities for the year.....	35
Logistical and administrative support to the EDPB .....	39
<b>EDPS-EDPB Joint opinions .....</b>	<b>40</b>
<b>Resources management.....</b>	<b>40</b>
<b>Human resources .....</b>	<b>40</b>
Development of employees, teams and of the organisation .....	40
Staff.....	41
<b>Budget.....</b>	<b>42</b>
Budget discharge .....	42
Budget allocation for 2024.....	42
Budget implementation .....	42
Draft budget for 2025 .....	43
<b>Finance.....</b>	<b>43</b>
Ex-ante.....	44
<b>Procurement and contracting .....</b>	<b>44</b>
<b>Missions' management .....</b>	<b>45</b>
<b>IT infrastructure and tools .....</b>	<b>46</b>
<b>Cybersecurity, Information Security, Physical Security and Business Continuity .....</b>	<b>47</b>

**Internal control..... 48**

**Control results..... 48**

        Effectiveness ..... 48

        Efficiency.....50

**Audit observations ..... 51**

        Internal Audit Service ..... 51

        European Court of Auditors..... 52

**Annual planning and risk management ..... 52**

**Internal control annual assessment ..... 52**

**Conclusions on the assurance..... 53**

**Declaration of assurance..... 53**

**Annexes ..... 55**

**Human resources at the EDPS/EDPB ..... 55**

**Budget in 2024 ..... 57**

**List of missions undertaken by the Supervisor in 2024 ..... 61**

## Abbreviations

AA	Administrative Arrangement
AAR	Annual Activity Report
ABAC	Accrual Based Accounting System
AEPD	Spanish Data Protection Authority
AFSJ	Area of Freedom, Security and Justice
AI	Artificial Intelligence
AIGO	Working Party on Artificial Intelligence Governance
AIWG	Working Group on Ethics and Data Protection in Artificial Intelligence
AMP	Annual Management Plan
AOD	Authorising Officer by Delegation
BCRs	Binding Corporate Rules
BfDI	Federal Data Protection Commissioner of Germany
CAI	Committee on AI
CBPR	Global Cross-Border Privacy Rules
CDEP	Committee on Digital Economy Policy
CEA	Coordinated Enforcement Action
CEF	Coordinated Enforcement Framework
CERT-EU	The Computer Emergency Response Team of the EU Institutions, bodies and agencies
CICED	Core International Crimes Evidence Database
CIS	Customs Information System
CJEU	Court of Justice of the European Union
CMS	Case Management System
CNIL	French Data Protection Authority
CoE	Council of Europe
CPDP	Computers, Privacy and Data Protection
CSAM	Child Sexual Abuse Material
CSC	Coordinated Supervision Committee
DDoS	Distributed Denial-of-Service
DFFT	Data Free Flow with Trust
DG	Directorate-General
DGA	Data Governance Act
DGP	Working Party on Data Governance and Privacy in the Digital Economy
DMA	Digital Market Act
DPA	Data Protection Authority
DPbDD	Data Protection by Design and Default
DPC	Digital Policy Committee
DPF	Data Protection Framework
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
ECA	European Court of Auditors
ECAS	European Commission Authentication Service
ECRIS-TCN	European Criminal Records Information System on non EU-nationals
EDIB	European Data Innovation Board
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EES	Entry/Exit System

EESSI	Electronic Exchange of Social Security Information
EMA	European Medicine Agency
ENISA	European Union Agency for Cybersecurity
EO	European Ombudsman
EP	European Parliament
EPPO	European Public Prosecutors' Office
EPSO	European Personnel Selection Office
ETIAS	European Travel Information and Authorisation System
EU	European Union
EUCI	EU Classified information
EUDPR	<a href="#">Regulation (EU) 2018/1725</a> 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
EUROCONTROL	European Organisation for the Safety of Air Navigation
EURODAC	European Asylum Dactyloscopy Database
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EUROSUR	European Border Surveillance System
EuSA	European School of Administration
Frontex	European Border and Coast Guard Agency
Garante	Italian Data Protection Authority
GDPR	' <a href="#">General Data Protection Regulation</a> ' 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
HoSG	Head of Secretary-General
HoU	Head of Unit
HR	Human Resources
HRBA	Human Resources and Budget Administration Unit
IAS	European Commission Internal Audit Service
ICC	Internal Control Coordinator
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
IMI	Internal Market Information
IOCC	Inter-Institutional Online Communication Committee
IOW	International Organisations Workshop
IPEN	Internet Privacy Engineering Network
IT	Information Technology
IWGDPT	International Working Group in Data Protection in Technology
JIT	Joint Investigation Team
JRC	Joint Research Centre
KPI	Key Performance Indicator

L&D	Learning and Development
LCO	Local Cybersecurity Officer
LISO	Local Information Security Officer
LLMs	Large Language Models
LSIT	Large Scale IT Systems
LSO	Local Security Officer
MEPs	Members of the European Parliament
MoU	Memorandum of Understanding
MS	Member State
MSCA	Marie Skłodowska-Curie Actions
NER	Named Entity Recognition
NGO	Non-Governmental Organisation
OCR	Optical Character Recognition
OECD	Organisation for Economic Co-operation and Development
OLAF	European Anti-Fraud Office
OSS	One stop shop
PATRICIA	‘Personal dATa bReach awareness In Cybersecurity Incident hAndling’
PEReN	Interdepartmental office operating under the joint authority of the French Ministers of Economy, Culture, and Digital Technology
PET	Privacy Enhancing Technology
PKI	Public Key Infrastructure
PMO	Paymaster Office of the European Commission
RAG	Retrieval-Augmented Generation
REA	Research Executive Agency
RoP	Rules of Procedure
RTOP	Restricted lapTOPs
SA	Supervisory Authority
SCG	Supervision Coordination Groups
SESAR	Single European Sky ATM Research 3 Joint Undertaking
SIS	Schengen Information System
SLA	Service Level Agreement
SMEs	Small and Medium-Sized Enterprises
SoA	Statement of Assurance
SPE	Support Pool of Experts
SR	Staff Regulation
SRB	Single Resolution Board
SSS	Staff Satisfaction Survey
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 Financial Regulation (Article 74.9<sup>1</sup>) stipulates that each authorising officer by delegation (AOD) shall submit an annual activity report (AAR) to their Union institution, together with financial and management information. This report shall present the achievements of their institution in relation to the resources used. It shall also be a management report on performance in the context of their task as AOD. This requirement is the logical consequence of paragraph 2 of this same article, which gives the AOD responsibility for internal controls.

In the annual activity report of the AOD, this latter must include a Statement of Assurance (SoA) based on their own judgment and on the information available in which the AOD:

- states that the information contained in the report gives a true and fair view;
- declares that the AOD has reasonable assurance that 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;
- confirms that the AOD is not aware of any matter not reported which could harm the interests of the institution.

## EDPS Highlights of the year

In 2024, with the entry into force of the **Artificial Intelligence (AI) Act**, the EDPS became the competent authority responsible for supervising EU institutions, bodies, and agencies (EUIBAs) that fall within the scope of this Regulation. Additionally, the EDPS assumed the roles of market surveillance authority, notifying body, and notifying authority for EUIBAs that fall under the AI Act. To fulfil its new obligations and tasks under the AI Act, which are carried out separately and without prejudice to its existing competences, tasks, powers, and independence under applicable data protection legislation, the EDPS established an AI Unit.

Regarding the exercise of EDPS powers in 2024, it is notable that the EDPS utilised its **investigative powers** to follow-up on, conduct, or finalise inspections into the processing of personal data by certain EUIBAs. The ongoing or closed investigations launched in 2023 encompass a range of subjects, demonstrating the EDPS's continued efforts to ensure compliance with data protection regulations.

The year 2024 marked the **EDPS' 20th anniversary**, two decades of protecting privacy and data protection. With this milestone came the inevitable need to reflect on the progress made, the mountains conquered, and lessons learned, serving as fuel to plan ahead, to tackle the challenges of tomorrow. This process, was necessary for the EDPS that has an ambitious mission and wishes to adapt and to keep up the pace with an ever-evolving digital landscape so that it is able to respond adequately to protect individuals' data protection rights.

Following this dynamic, the year 2024 was dedicated to preparing the data protection landscape of tomorrow by analysing the past, current and possible future dynamics between data protection, privacy, technology, policy and other fields. To achieve this, the EDPS chose to base its anniversary on four key pillars - all designed to highlight the importance and impact of data protection.

The first pillar was composed of **a book** and **a timeline** that analysed key data protection **milestones** and the EDPS' influence and history in this remit over the last two decades, as well as an in-depth analysis of what is yet to come.

---

<sup>1</sup> Regulation 2018/1046: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1046>



To inform about EDPS work as a data protection authority going forward, the organisation must also be able to learn from others. The second pillar comprised **20 talks with leading voices** from around the world who share their unique perspective on how data protection and privacy shapes their respective fields.

With a view of modernising the EDPS' approach to anticipate and tackle future challenges, the third pillar included **20 initiatives** aimed at further emboldening individuals' fundamental rights.

The fourth pillar is the **European Data Protection Summit - Rethinking Data in a Democratic Society**, which took place on 20 June 2024, in Brussels, Belgium. During this event, the EDPS fostered dynamic and open discussions on the role of privacy and data protection in modern democracies by examining, in particular, the role of a state at a time of an ever-growing collection of information about citizens.

With these four pillars, the EDPS, as a **responsible** and **forward-looking data** protection authority, has managed to anticipate the challenges and opportunities ahead for equipping itself with enforceable regulatory tools that protect individuals' personal data, in an era where data is pivotal in shaping the digital landscape, businesses, governments and other entities.

## Strategy

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

The EDPS Strategy for 2020-2024<sup>2</sup> focuses on three pillars: **Foresight**, **Action** and **Solidarity** to shape a safer, fairer and more sustainable digital future.

- **Foresight:** the EDPS commitment to being a smart institution that takes the long-term view of trends in data protection and the legal, societal and technological context.
- **Action:** proactively develop tools for EUIBAs to be world leaders in data protection. To promote coherence in the activities of enforcement bodies in the EU with a stronger expression of genuine European solidarity, burden sharing and common approach.
- **Solidarity:** the EDPS belief is that justice requires privacy to be safeguarded for everyone, in all EU policies, whilst sustainability should be the driver for data processing in the public interest.

## Key performance indicators

The EDPS uses a number of key performance indicators (KPIs) for monitoring performance as set by the main objectives of the EDPS Strategy<sup>3</sup>. The KPI scoreboard below contains a brief description of each KPI and the results on 31 December 2024. These results are measured against initial targets, or against the results of the previous year.

In 2024, the organisation met or surpassed the targets set in all KPIs, except one, confirming the positive trend in implementing our strategic objectives throughout the year. KPI 7, on followers on EDPS social media, did not fully meet the set target due to the reduced growth in the number of followers on X (ex-Twitter). This might have resulted from a general decline in the number of people active on this social media.

---

<sup>2</sup> EDPS Strategy for 2020-2024: [https://www.edps.europa.eu/sites/default/files/publication/20-06-30\\_edps\\_shaping\\_safer\\_digital\\_future\\_en.pdf](https://www.edps.europa.eu/sites/default/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf)

<sup>3</sup> KPIs are regularly revised to ensure that performance metrics adapt to developments in EDPS activities.

KEY PERFORMANCE INDICATORS		Results 31.12.2024	Target 2024	
<b>KPI 1</b> <b>Internal indicator</b>	Number of cases, incl. publications, on technology monitoring and on promoting technologies to enhance privacy and data protection organised or co-organised by EDPS	10 cases	5 cases	
<b>KPI 2</b> <b>Internal &amp; External Indicator</b>	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8 activities	8 activities	
<b>KPI 3</b> <b>Internal Indicator</b>	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 contribution	38 cases	10 cases	
<b>KPI 4</b> <b>External Indicator</b>	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	17 files	10 files	
<b>KPI 5</b> <b>External Indicator</b>	Number of Article 42 opinions and joint EDPS-EDPB opinions issued in response to EC legislative consultation requests	25 Opinions	25 opinions	
<b>KPI 6</b> <b>External Indicator</b>	Number of audits/visits carried out physically or remotely	10 audits/visits	5 different audits/visits	
<b>KPI 7</b> <b>External Indicator</b>	Number of followers on the EDPS social media accounts <sup>4</sup>	LI: 82,8 k X: 28,8 k YT: 3,4 k Instagram: 0,3 k	Results of previous year <sup>5</sup> + 10%	
<b>KPI 8</b> <b>Internal</b>	Occupancy rate of establishment plan	98.8%	90%	

<sup>4</sup> Number of followers on the EDSP social media accounts: Twitter, LinkedIn, YouTube, Instagram.

<sup>5</sup> Results of the previous year: 2023 result - 110 293.

Indicator				
KPI 9	Budget implementation	96%	90%	
Internal Indicator				

## Operational achievements

### European Data Protection Supervisor

#### Supervisory tasks

In 2024, the EDPS continued to supervise European Union institutions, bodies, offices, and agencies (EUIBAs) on their compliance with the EU's data protection legal framework, particularly Regulation (EU) 2018/1725<sup>6</sup> (the 'EUDPR'). As outlined in the 2020-2024 Strategy, the EDPS remains committed to supporting EUIBAs in setting an example for safeguarding digital rights and responsible data processing practices. The following section describes several initiatives undertaken by the EDPS in 2024.

To enhance and optimise its supervisory tasks, the EDPS initiated the development of a **new supervision and enforcement strategy** in 2024. This effort will continue in 2025 with more detailed planning for various activities, including audits, investigations, and complaint handling, taking into account the transition to a new EDPS mandate. Effective and consistent supervision and enforcement of data protection rules require a clear, strategic approach that outlines objectives, priorities, and specific actions to ensure compliance. A supervision and enforcement strategy provides a framework for monitoring and assessing compliance across organisations, enabling the EDPS to identify high-risk processing activities, standardise practices, and allocate limited resources where they can have the most significant impact.

By promoting accountability and transparency, the strategy supports the uniform application of rules, fostering trust among data subjects. Furthermore, it facilitates the timely detection and rectification of breaches, establishing a structured pathway for penalties and corrective actions that uphold data protection principles. This approach ensures that EUIBAs are held to consistent standards and that data subjects' rights are comprehensively safeguarded.

---

<sup>6</sup> [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.

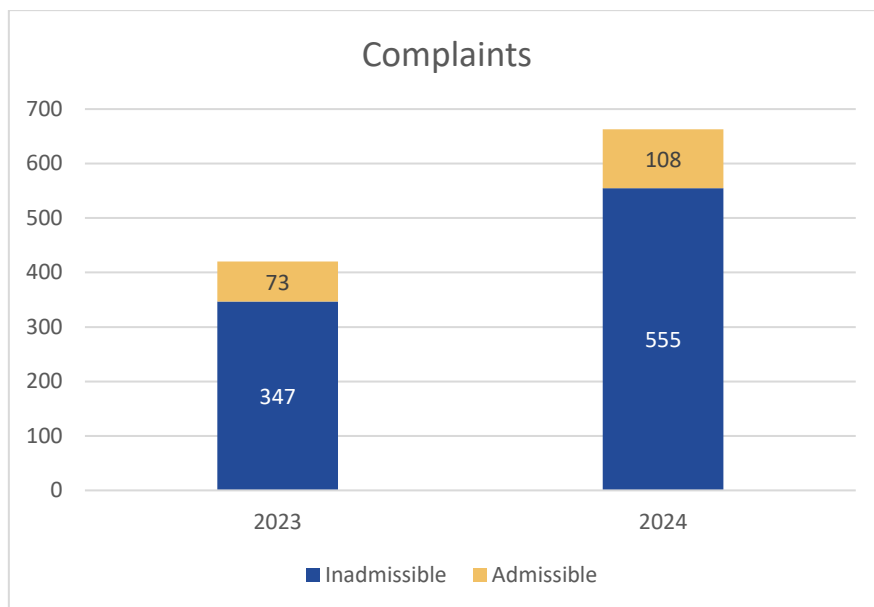
## Supervising all European Institutions, bodies, offices and agencies

### 1. Complaints and investigations

#### A. Complaints

The EDPS is responsible for investigating complaints from individuals concerning the processing of their personal data by EUIBAs. Additionally, staff members of EUIBAs may also submit complaints to the EDPS regarding alleged breaches of the EUDPR, regardless of whether the matter involves the processing of their own personal data or not.

In 2024, the EDPS received **663 complaints**, i.e. 202 more compared to 2023. Out of the 663 complaints received, **108** were **admissible** and **555** **inadmissible**. During the reporting year, the EDPS finalised 77 admissible complaint cases, which represents an increase of 33% compared to 2023. In addition, the EDPS responded to all 555 inadmissible complaints received.



The admissible complaint cases of 2024 varied in complexity, both in substance (e.g., the nature of processing or issues raised) and procedure (e.g., involvement of multiple EUIBAs, extensive exchanges with the parties, identifying links between multiple complaints from the same complainant, or significant changes required after preliminary assessment), or in both aspects. Overall, many complaints resulted in enhanced personal data protection within the EUIBAs and for EU citizens.

Two notable cases involved the European Commission:

In 2024, the EDPS issued a decision on three complaints concerning the remotely proctored (monitored) testing in selection procedures conducted by the **European Personnel Selection Office (EPSO)** through an external contractor in the course of 2023<sup>7</sup>. The EDPS found that EPSO had infringed several provisions of the EUDPR<sup>8</sup>, and issued a reprimand to EPSO.

<sup>7</sup> Summary of EDPS' decision against EPSO at: [https://www.edps.europa.eu/system/files/2025-01/24-11-27\\_summary-epso-decision\\_en.pdf](https://www.edps.europa.eu/system/files/2025-01/24-11-27_summary-epso-decision_en.pdf)

<sup>8</sup> (i) Article 5(1)(d) EUDPR by incorrectly relying on consent as legal basis for the processing; (ii) Article 10(2) EUDPR by processing biometric data for the purposes of uniquely identifying candidates without any legal basis; (iii) Articles 4(1)(a), 14, 15 and 16 EUDPR by not providing fair, transparent and sufficient information to candidates; (iv) Article 29(3)(a) EUDPR and Article 46 EUDPR by not being in control of the processing operations conducted on its behalf by its processor and sub-processors, which resulted in transfers of candidate data to third countries without any transfer tool.

In 2024, the EDPS issued a decision on a complaint concerning the **EC's targeted advertising campaign** on the social media **platform X**. The campaign, which ran in September 2023, aimed to promote the EC's legislative proposal on preventing and combating child sexual abuse. The complainant alleged that his personal data had been unlawfully processed in this context. As part of the campaign, the EC targeted X users over the age of 18 from certain EU Member States. The EDPS investigation revealed that the targeting also involved including and excluding users based on their interactions with posts containing specific keywords set by the EC. Some of these keywords related to political parties, politicians, Eurosceptic and/or nationalistic views, and religious beliefs. Additionally, the campaign targeted users with interests similar to key accounts selected by the EC. EDPS found that the EC had violated several provisions of the EUDPR by unlawfully processing the complainant's personal data, including special categories of data such as political opinions and religious beliefs, without a valid legal basis. Considering that the processing was no longer ongoing, EDPS issued a reprimand for these infringements.

## B. Investigations

EDPS investigations assess whether EUIBAs have breached data protection rules, adhering to proportionality, fairness, and core values of impartiality, integrity, transparency, and pragmatism. Investigations may be initiated based on third-party reports or at EDPS's discretion. Before launching a formal investigation, a pre-investigation may be conducted to evaluate compliance and the credibility of allegations. In case of strong suspicion on infringement of data protection rules by a EUIBA, the EDPS may carry out a formal investigation.

In line with the EDPS Strategy<sup>9</sup>, the organisation prioritised investigations into EUIBAs' use of **cloud-based** and other **emerging technologies**, particularly those involving **data transfers outside the EU/EEA**. Investigations, as EDPS' most important tool for supervision and enforcement, involve legal and technical experts and follow a structured process, including evidence gathering, inspections, and preliminary assessments. Given their complexity, formal investigations require significant resources.

Here is a selection of the most notable cases handled during 2024:

**Profiling in public access applications:** a pre-investigation found that a EUIBA's detection of circumvention in application queuing systems constituted profiling under the EUDPR. EDPS recommended informing data subjects and assessing the need for carrying out a data protection impact assessment.

**Automated decision-making** in trainee selection: a pre-investigation was launched into whether an EUIBA's (pre)selection process relied solely on automated decision-making and whether safeguards and transparency measures were in place. This investigation is still ongoing.

**EC's use of Microsoft 365**<sup>10</sup>: An investigation found multiple EUDPR violations, particularly regarding purpose limitation and international data transfers. EDPS ordered the EC to suspend all data flows to Microsoft and its affiliates outside the EU/EEA by 9 December 2024, and ensure compliance with EUDPR. In December 2024<sup>11</sup>, the EDPS initiated the follow-up on the compliance of the EC's use of Microsoft 365, still ongoing. The EDPS worked on this investigation from May 2021 to March 2024, which was particularly complex given the high level of technical and legal expertise required as well as the amount of information and data processing activities that needed to be taken into account.

---

<sup>9</sup> EDPS' Strategy: [https://www.edps.europa.eu/press-publications/publications/strategy\\_en](https://www.edps.europa.eu/press-publications/publications/strategy_en)

<sup>10</sup> See the EDPS' decision of 8 March 2024 following investigation into the European Commission's use of Microsoft 365: [https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365\\_en.pdf](https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf)

<sup>11</sup> See related press release: [https://www.edps.europa.eu/system/files/2024-12/EDPS-2024-12-Decision-Microsoft\\_EN.pdf](https://www.edps.europa.eu/system/files/2024-12/EDPS-2024-12-Decision-Microsoft_EN.pdf)

With regard to the **Area of Freedom, Security and Justice**, the EDPS **reprimanded**<sup>12</sup> the **European Border and Coast Guard Agency** (Frontex) for **unlawfully transmitting personal data** of cross-border crime suspects to **Europol** without assessing necessity, violating Regulation (EU) 2019/1896<sup>13</sup>.

Photography<sup>14</sup> by Frontex officers: Following non-governmental organisations (NGO) allegations, EDPS found insufficient evidence of EUDPR breaches but identified risks due to the lack of a policy on photographing apprehended individuals. Recommendations included a clear prohibition policy and strengthened DPO investigative capacity.

Where appropriate, the EDPS may investigate EUIBAs' compliance with the EUDPR and the **ePrivacy Directive**, either in response to complaints or on its own initiative.

**EUIBAs website compliance**<sup>15</sup>: EDPS continued five investigations into EUIBAs' website practices, focusing on third-party components and consent requests. Given their broader implications, EDPS is collaborating with other DPAs to develop a unified approach.

**Personal data breaches**: EDPS followed up on high-risk<sup>16</sup> breaches, issuing recommendations and considering audits or investigations where necessary. As an example, a pre-investigation into security measures for the EC's FORMS tool was conducted and subsequently closed after a thorough examination of the security measures applied.

The **steady increase** in the **processing of personal data** by EUIBAs and the enhanced **procedural and technical complexity** of the information systems that support them influence the duration and the complexity of EDPS' investigations as well as increase the need to cooperate with other DPAs working on similar matters. This continues to have an impact on the limited resources available in the area of supervision in the EDPS.

### C. Court cases against EDPS' decisions and related appeals

EUIBAs, as well as their processors (including those that are not EUIBAs) may initiate proceedings before the General Court against EDPS decisions in complaints and investigation cases. In addition, complainants have the right to bring an action before the General Court against a decision or inaction of the EDPS in complaints cases. The judgments of the General Court are subject to appeal before the Court of Justice of the EU (CJEU).

In 2024, two court cases were pending before the General Court, challenging an EDPS decision, and two appeals were pending before the CJEU:

In June 2024, the **EC** and **Microsoft** brought actions before the General Court against the EDPS decision of 8 March 2024 (see [above](#)). In their applications, the EC<sup>17</sup> and Microsoft<sup>18</sup> contest all EDPS findings of

---

<sup>12</sup> This decision closed the investigation launched following the audit carried out by the EDPS in October 2022 on Frontex's activities when assisting Member States at the EU external borders in joint operations. The decision also addressed the issues raised in the context of the EDPS' pre-investigation opened in 2023 regarding the processing in debriefing reports of NGO staff' personal data and their further transmission to Europol.

<sup>13</sup> Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 <https://eur-lex.europa.eu/eli/reg/2019/1896/oj/eng>

<sup>14</sup> The allegations concerned reports that Frontex Standing Corps members have, on multiple instances, photographed individuals during apprehension, with the officers' smartphones, and outside of formal identification and fingerprinting procedures.

<sup>15</sup> These investigations concern a complex topic and various allegations of potential infringements of the EUDPR and Article 5(3) of Directive 2002/58/EC, necessitating several evidence collections to gather relevant information. As such, these cases require a detailed analysis of whether the EUIBAs concerned have complied with the relevant rules.

<sup>16</sup> High risk cases are considered situations where the data breaches lasted a very long time or were detected very late, affected a high number of individuals, involved several EUIBAs or were due to cyber-attacks flagged by CERT-EU or due to serious omissions in measures in place at the EUIBA.

<sup>17</sup> Commission v EDPS - Case T-262/24:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=287804&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=26202684>

<sup>18</sup> Microsoft Ireland Operations v EDPS – Case T-265/24:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=287806&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=26202797>

infringement and all corrective measures imposed, and sought to have the decision annulled. The EDPS maintains its decision and is defending it in the ongoing court proceedings. Neither the EC nor Microsoft requested interim measures from the General Court. The two court cases do not suspend the execution of the EDPS decision which remains fully applicable.

In April 2023, the General Court<sup>19</sup> issued a judgement<sup>20</sup> concerning the **Single Resolution Board's** (SRB) handling of personal data shared with an external consultant. In July 2023, the **EDPS appealed**<sup>21</sup> this judgement and a hearing before the CJEU was held in November 2024. The EDPS sought to annul the judgment, arguing that the General Court had misinterpreted EUDPR in two key areas:

- first, of Article 3(1) and 3(6) as interpreted by the case-law of the CJEU for having required the EDPS to assess whether the information at stake in the case was personal data taking the perspective of the recipient and by omitting to give consideration to the notion of pseudonymisation and
- second, of Article 4(2) and 26(1) of EUDPR by omitting to give any consideration to the principle of accountability and having found that the EDPS should have proven that the SRB had effectively anonymised the personal data it was processing.

A final decision is still pending.

On 16 November 2023, the EDPS lodged an appeal before the CJEU requesting that the General Court's order<sup>22</sup> of 6 September 2023 is set aside. The General Court had found that the EDPS has no standing to request the annulment of two provisions of the amended Europol Regulation and dismissed<sup>23</sup> the EDPS action as inadmissible. These two new provisions have an impact on personal data operations carried out by Europol and the EDPS considers this may affect legal certainty for individuals' personal data and interfere with the independence of the EDPS.

#### D. Procedural work items related to complaints and investigations

Alongside its investigatory activities, the EDPS in 2024 focused on **refining** and **updating** its **procedures**. Key initiatives included reviewing investigation methodologies, developing a manual on access to the file, enhancing litigation preparedness, updating the internal complaints case manual, and improving hearing recording and transcription processes.

A significant change was the **revision** of specific provisions in the **EDPS Rules of Procedure** (RoP)<sup>24</sup>, strengthening the right to be heard with the abolishment of the review mechanism and the introduction of preliminary assessments. Since July 2024, controllers and processors have the opportunity to share their views before the EDPS takes a decision that could negatively affect them. This assessment outlines the established facts, supporting evidence, initial legal analysis, potential infringements, and any corrective measures under consideration. Complainants are also given the opportunity to present their views before a decision rejecting their complaint, in whole or in part, is issued. This procedural safeguard enhances fairness, transparency, and efficiency in complaints handling.

These updates require substantial time and resources. With new tasks emerging - such as refining procedures for investigations, corrective measures (including fines), and personal data breach follow-ups - further procedural developments are anticipated.

---

<sup>19</sup> Eighth Chamber, Extended Composition

<sup>20</sup> Case T-557/20: <https://curia.europa.eu/juris/liste.jsf?num=T-557/20&language=en>

<sup>21</sup> European Data Protection Supervisor v. Single Resolution Board C-413/23 P: <https://curia.europa.eu/juris/liste.jsf?num=C-413/23&language=en>

<sup>22</sup> Case C-698/23 P: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62023CN0698>

<sup>23</sup> Case T-578/22: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022TN0578>

<sup>24</sup> Revision of the EDPS' Rules of Procedure: [https://www.edps.europa.eu/system/files/2024-09/oj\\_l\\_202402022\\_en\\_0.pdf](https://www.edps.europa.eu/system/files/2024-09/oj_l_202402022_en_0.pdf)



## 2. Cooperation with data protection authorities in supervision and enforcement of data protection rules

In 2024, the EDPS cooperated with Data Protection Authorities (DPAs) both within and outside of the EU/EEA, as well as in international fora on five cases to supervise and enforce data protection legislation. This cooperation involved sharing practical information on findings and actions taken by the EDPS and other DPAs. In addition, within the EU/EEA, the EDPS worked with DPAs through the European Data Protection Board (EDPB), providing input based on its supervisory and enforcement experience to support EDPB guidance and dispute resolution. In 2024, the EDPS participated in the EDPB's **Coordinated Enforcement Action** (CEA) on the right of access to personal data, conducting a survey with EUIBAs' Data Protection Officers (DPOs) (see more information [here](#)). Meanwhile, it continued collaborating on the 2023 CEA on DPO designation, contributing to the EDPB's report and publishing its own stand-alone report in January 2024. The EDPS also prepared for the 2025 CEA on the right to erasure.

The EDPS contributed to EDPB opinions on data controller obligations and Article 5(3) of Directive 2002/58/EC<sup>25</sup>. Additionally, it played a key role in drafting EDPB guidelines on Article 14 of the Law Enforcement Directive, leveraging its experience handling Europol-related complaints.

Cooperation with EU supervisory authorities is crucial in the **Area of Freedom, Security, and Justice** (AFSJ), where increasing data exchanges between EUIBAs and national authorities require coordinated supervision. Under Article 62 EUDPR, the EDPS and national supervisory authorities (SAs) must work together to oversee large-scale IT systems and EUIBAs. This is primarily conducted through the **Coordinated Supervision Committee** (CSC), which is gradually absorbing Supervision Coordination Groups (SCGs).

In 2024, the EDPS actively engaged in CSC activities, including:

- Assuming CSC coordination in July 2024 for a two-year term, allowing for new working methods to enhance efficiency.
- Drafting a guidance note on cooperation in handling Europol complaints, adopted by the CSC.
- Leading coordinated actions to assess Europol's processing of personal data on minors under 15 designated as suspects, culminating in a joint report.
- Monitoring ETIAS Development: the interoperability framework poses data protection challenges due to complex data flows and multiple controllers at EU and national levels, requiring stronger coordination between the EDPS and national DPAs. In 2024, the CSC's ETIAS working group analysed legal interpretations of the ETIAS Regulation, participated in Data Protection Impact Assessment (DPIA) meetings, and raised data protection concerns in a letter to the European Commission's Directorate-General (DG) for Home Affairs.

During the reporting year, the EDPS also continued participating in Supervision Coordination Groups (SCGs), which oversee **large-scale EU IT systems**. As regulatory updates shift oversight to the CSC only two SCGs remain: one on Eurodac, which supports asylum and crime prevention, and another for the Customs Information System (CIS). The Visa Information System (VIS) transitioned to CSC supervision in 2024.

While cooperation requires significant resources, it fosters a shared understanding of data protection challenges across the EU/EEA and beyond, ensuring effective supervision of similar processing activities and technologies used in the public interest. More information regarding the SCGs and their activities are published on the respective webpages of the CIS<sup>26</sup> and Eurodac<sup>27</sup> on the relevant EDPS webpage; see also [here](#).

---

<sup>25</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32002L0058>

<sup>26</sup> Webpage of CIS: [https://www.edps.europa.eu/data-protection/supervision-coordination/customs-information-systems\\_en](https://www.edps.europa.eu/data-protection/supervision-coordination/customs-information-systems_en)

<sup>27</sup> Webpage of Eurodac: [https://www.edps.europa.eu/data-protection/european-it-systems/eurodac\\_en](https://www.edps.europa.eu/data-protection/european-it-systems/eurodac_en)



### 3. Supervisory opinions and guidance

#### A. Strategic actions concerning transfers of personal data outside of EU/European Economic Area (EEA)

Following the Court of Justice of the European Union's (CJEU) "Schrems II" judgment<sup>28</sup>, the EDPS developed various initiatives in the area of international transfers and established the **EDPS' Schrems II Strategy**<sup>29</sup>. The Strategy aims to ensure and monitor compliance of EUIBAs with the requirements of the CJEU concerning transfers of personal data to non-EU/EEA countries, building on cooperation and accountability of controllers as well as on the use of EDPS corrective powers. Three types of actions were pursued in parallel, including investigations, transfer authorisations, advisory work, and guidance to assist the EUIBAs in discharging their duty of accountability. For such an extensive monitoring of EUIBAs compliance with EUDPR, the EDPS updated the guidance on transfers in its website, in particular information such as the obligation to notify the EDPS on the categories of transfers carried out under Articles 48 and 50 of EUDPR.

The **EU-US Data Protection Framework (DPF)** is key development to enabling the free flow of personal data between the EEA and the U.S. The EDPS has closely monitored its implementation and contributed to the first DPF review<sup>30</sup> in 2024. Transfers to U.S. entities not on the Data Privacy Framework List require additional safeguards under the EUDPR.

In 2024, the EDPS published its **Model Arrangement (Model)** for transfers of personal data<sup>31</sup> from EUIBAs to International Organisations. The Model helps EUIBAs comply with EUDPR, by ensuring data transfers uphold core data protection principles and necessary safeguards, maintaining a protection level equivalent to EU law. While arrangements based on the Model still require EDPS approval, its use simplifies the process, benefiting both parties and the individuals concerned.

In addition, the EDPS issued a decision<sup>32</sup> on the use of the amended administrative arrangement between the **Single European Sky ATM Research 3 Joint Undertaking ('SESAR')** and **Eurocontrol** in the context of Eurocontrol's in-kind contributions to SESAR. The updated administrative arrangement and new Eurocontrol data protection rules ensure a level of data protection equivalent to that guaranteed by the EUDPR.

The EDPS has been also working on other issues connected with international transfers on request of some EUIBAs, including the use of derogations under Article 50 EUDPR in specific cases.

#### B. Data protection audits

The EDPS conducts regular data protection audits as part of its authority over data protection for EUIBAs. In 2024, the Annual Audit Plan included on-site visits to assess various processing activities, such as health data processing, retention periods, and research involving minors.

---

<sup>28</sup> Case C-311/18: <https://curia.europa.eu/juris/liste.jsf?num=C-311/18>

<sup>29</sup> Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling, 29 October 2020: [https://www.edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en)

<sup>30</sup> Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0451>

<sup>31</sup> EDPS' Model Administrative Arrangement for transfers of personal data from EUIs to International Organisations: [https://www.edps.europa.eu/data-protection/our-work/publications/international-transfers/2024-07-31-edps-model-administrative-arrangement-transfers-personal-data-euis-international-organisations\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/international-transfers/2024-07-31-edps-model-administrative-arrangement-transfers-personal-data-euis-international-organisations_en)

<sup>32</sup> EDPS' Decision the use of the amended administrative arrangement between the SESAR and the Eurocontrol in the context of Eurocontrol's in-kind contributions to SESAR: [https://www.edps.europa.eu/data-protection/our-work/publications/international-transfers/2024-06-28-edps-use-amended-administrative-arrangement-between-sesar-and-eurocontrol-context-eurocontrols-kind-contributions-sesar\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/international-transfers/2024-06-28-edps-use-amended-administrative-arrangement-between-sesar-and-eurocontrol-context-eurocontrols-kind-contributions-sesar_en)

In 2024, the EDPS carried out **three audits**:

1. European Commission, General Secretariat of the Council, and the European Parliament: focusing on retention periods for medical documents, which revealed shortcomings and led to recommendations for improvement.
2. Europol's in-house medical service: identifying issues with processing activities, individual rights, and security, resulting in a number of recommendations for improving compliance with the EUDPR.
3. European Commission's Joint Research Centre (JRC): examining the processing of children's personal data in research projects, highlighting areas for improvement in lawfulness, transparency, and security.

Additionally, the EDPS:

- Issued a report on an in-depth inspection<sup>33</sup> at Europol, finding shortcomings and issuing 23 recommendations for improvement.
- Conducted an audit at Eurojust to verify compliance with the EUDPR and Eurojust Regulation, focusing on operational personal data processing in the Core International Crimes Evidence Database (CICED); conducted a follow-up on prior consultations of the CICED stages and other activities.
- Carried out follow-up activities on previous audits and participated in Schengen evaluations in the field of data protection as observer.

### C. Supervisory opinions and guidance

EUIBAs may consult the EDPS for guidance on planned processing operations and data protection compliance. Depending on the complexity, advice is given via DPO hotline calls, informal guidance, or formal letters. In some cases, consultation is mandatory, such as for internal rules restricting data protection rights or extra-EU transfers requiring prior authorisation. The EDPS can also issue own-initiative opinions.

In total, during 2024 the EDPS issued advice on **26 consultations**, including one prior consultation under Article 40 EUDPR. The EDPS also issued **14 supervisory opinions** on various topics. Here are some key examples:

- **Opinion on the Data Protection Impact Assessment for the EudraVigilance Signal and Safety Analytics Platform as requested by the European Medicines Agency (EMA)**

With this opinion<sup>34</sup> the EDPS assessed whether the EMA proposed mitigating measures adequately address the high risks associated with the EudraVigilance Signal and Safety Analytics Platform. The EDPS concludes that the EMA's mitigating measures are sufficient, provided that recommendations as identified in the opinion, are implemented.

- **Opinion on biometric attendance system for members of the European Parliament**

In December 2024, the EDPS published a supervisory opinion regarding the European Parliament's plan to use biometrics to attest of MEPs' attendance, for daily allowances payments. The EP proposed a 2-year transitional period with a badge-based system and optional fingerprint scanning. The EDPS found that the EP cannot rely on both consent and public interest as lawful grounds for processing biometric data.

---

<sup>33</sup> Focus on the processing of Passenger Name Records data, Europol's access to the Visa Information System and the implementation of Article 18(6a) and 18a of Regulation (EU) 2016/794 with regard to the processing of large datasets.

<sup>34</sup> Issued by the EDPS in accordance with Article 40(2) EUDPR following a prior consultation request from the European Medicines Agency.

Instead, the EDPS recommended relying solely on consent during the transitional period, as fingerprint scanning is voluntary. This ensures fairness and legal certainty for data subjects, allowing them to withdraw consent and stop biometric data processing. Once the transitional period ends and the fully biometric system is in place, public interest can be relied upon. The EDPS also provided recommendations to clarify the legal basis in Union law, ensuring it is clear, precise and foreseeable.

- **Opinion on restrictions of certain rights of data subjects in relation to the processing by the European Commission for the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065**

In this opinion, issued by the EDPS in October 2024, recommendations are made to ensure the compliance with the EUDPR. In a nutshell, the recommendations request including a reference to the right to lodge a complaint with the EDPS and involving the DPO in assessing the necessity and proportionality of restricting data subject rights

- **Opinion on retention periods of personal data for Marie Skłodowska-Curie**

The opinion of August 2024, regarding the European Research Executive Agency (REA) request to extend retention periods for personal data of Marie Skłodowska-Curie Actions (MSCA) candidates and funded researchers for historical and scientific research and statistical purposes, as well as for the purposes of detecting plagiarism and any other scientific misconduct.

The EDPS recommended a specific, longer but not indefinite retention period for historical research purposes, combined with regular reviews to ensure only valuable data is preserved and implementation of safeguards, such as data minimisation through anonymisation or pseudonymisation.

- **Opinion on integrating the EC's Pay Master Office (PMO) into the Electronic Exchange of Social Security Information (EESSI) for the exchange of data regarding social security benefits**

In this opinion, issued in February 2024, the EDPS concluded that: i) data transmission via EESSI<sup>35</sup> between the PMO<sup>36</sup> and national authorities is necessary for performing a task carried in the public interest, ii) the Commission should establish an explicit legal basis for PMO to exchange social security data via EESSI, iii) the Commission should ensure appropriate safeguards for individuals' fundamental rights and interests, iv) the Commission should be considered as a controller, not a processor, if it influences the purpose(s) and means of the processing operation through the EESSI governance structure.

- **Opinion on Commission's use of staff mobile numbers**

In November 2024, the EDPS issued an opinion on a draft Commission decision on the means of urgent internal communication. The draft decision provides that staff members and other persons working for it ('staff') may be contacted on their mobile for three purposes: i) for security and safety, ii) for business continuity, or iii) for duly justified work-related purposes<sup>37</sup>.

The EDPS made several recommendations, calling the EC to update its proposal with the following actions: specifying the purpose for contacting staff members in line with Article 4(1)(b) of the EUDPR, defining conditions for assessing what constitutes an "emergency" that justify contacting staff on their private numbers, while respecting their right to disconnect<sup>38</sup>, clarifying the scope and extent of contacting staff on their private numbers in case of emergency, analysing whether using corporate phone

---

<sup>35</sup> The EESSI is a decentralised information system established to facilitate the cross-border exchange of personal data relating to social security issues between the 32 EESSI participating countries (EU member states together with EEA countries, Switzerland and the United Kingdom).

<sup>36</sup> The PMO is an internal Commission department responsible for the financial entitlements of staff of the Commission and certain other EU Institutions.

<sup>37</sup> In accordance with Article 55(1) of the Staff Regulations, which provides that "Officials in active employment shall at all times be at the disposal of their institution".

<sup>38</sup> As included in Article 5 of Commission Decision C(2022) 1788.

numbers would be less intrusive than private numbers and ensuring that private phone numbers are permanently deleted when a staff member leaves the service.

- **Guidance on confidentiality claims during Commission anti-trust procedures**

The EDPS provided informal advice to the European Commission's DG Competition on updating its guidance for handling confidentiality claims during anti-trust procedures. Such advice concerned the assessment of claims for redaction of personal data based on data protection grounds. The EDPS emphasised that the guidance should align with its EDPS opinion on the processing of personal data in the context of competition law investigations<sup>39</sup>.

As regards the EUIBAs operating in the **Area of Freedom, Security and Justice**, the EDPS provided advice/guidance with regard to:

- New ways of cooperation between Europol and Member States (MSs) in the production of operational analysis, emphasising the need for clear data protection responsibilities and task allocation. Regarding a new tool granting MSs direct access to Europol's datasets, the EDPS stressed that joint operational analysis would qualify as a form of joint controllership, necessitating a defined agreement on personal data responsibilities between Europol and MSs. Consequently, the EDPS recommended a formal arrangement to secure effective data protection guarantees in these new **joint processing environments**.
- New tools for the law enforcement and judicial authorities. In the field of **biometrics**, the EDPS issued guidance focusing on the processing of facial recognition technology, emphasising the need for strict necessity and proportionality. The EDPS assessed the use of facial recognition technology in cases involving the connection of various series of child sexual abuse material (CSAM) and determined that the technology is reliable and fair, with no apparent biases that could lead to misidentification or unequal treatment. The EDPS also addressed the use of **artificial intelligence (AI) tools** in law enforcement, stressing the importance of trustworthy, fair, and unbiased tools. To ensure compliance with data protection principles, the EDPS recommended caution while using AI tools, separating large datasets, and implementing strong oversight measures to prevent bias and misidentification.
- **Transfers. Europol** consulted the EDPS on revising its model working arrangement for transferring information, including personal data, to third countries. The EDPS issued an opinion emphasising that while working arrangements can outline procedures and mechanisms for data processing, they cannot *per se* serve as a legal basis for personal data transfers. Europol must ensure that any transfer complies with the Europol Regulation, specifically Article 25, which defines the legal instruments allowing such transfers. This is particularly crucial when relying on derogations, given their exceptional nature. **Eurojust** also sought EDPS guidance on using **Joint Investigation Team (JIT)** agreements for transferring operational personal data to third countries. The EDPS found that the proposed data protection clauses do not qualify as an international agreement, as these are defined under Article 58(1)(a) of Eurojust Regulation. Instead, a case-by-case assessment is required to determine whether the proposed clauses provide adequate safeguards under Article 58(1)(b). At the same time, the EDPS acknowledged that the clauses incorporate essential data protection elements, making them a valuable addition to any JIT agreement and contributing to the protection of data subjects' rights.
- **European Border Surveillance System (EUROSUR)**. In 2024, the EDPS issued an opinion on the concepts of personal data and of the controllership as well as of the data protection legal framework applicable to

---

<sup>39</sup> Supervisory opinion on the processing of personal data in the context of competition law investigations: [https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2022-05-20-opinion-processing-personal-data-context-competition-law-investigations\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2022-05-20-opinion-processing-personal-data-context-competition-law-investigations_en)

Frontex's activities carried out in the context of the EUROSUR<sup>40</sup>. In his opinion, the EDPS considered that ships and aircraft identification numbers are personal data when processed by Frontex in the context of EUROSUR according to Article 89(2) of Regulation (EU) 2018/1796. The EDPS identified Frontex as the controller for processing personal data for *European situational picture* and Member States (MSs) for their *national situational picture*. Frontex and MSs are joint controllers for *specific situational pictures* established and maintained alone and/or together. The EDPS also identified Frontex as the controller for personal data derived from the EUROSUR fusion services. The EDPS concluded that EUROSUR's personal data processing falls under the EUDPR.

- **European Travel Information and Authorisation System (ETIAS).** ETIAS will process millions of visa-exempt travellers' data annually, involving sensitive processing operations like automated checks against law enforcement databases, watch listing and algorithmic profiling. Due to its complex multi-controller framework and shared responsibilities between MSs and EU agencies<sup>41</sup>, the EDPS has closely monitored its implementation. In 2024, the EDPS stepped up cooperation with ETIAS stakeholders to ensure data protection compliance by design and by default, participating in Frontex-led working groups and advising on non-discrimination and effective remedies as member of the ETIAS Fundamental Rights Guidance Board.

## Data Protection Audits of Large-scale IT Systems

Following legal requirements<sup>42</sup>, the EDPS ensures a personal data protection audit of the Management Authority's (eu-LISA) is carried out at least every four years for the Schengen Information System (SIS II) and Visa Information System (VIS) and every three years for the European Asylum Dactyloscopy Database (EURODAC). The results of the 2023 SIS audit were announced in 2024.

In 2024, the EDPS audited of the Large Scale IT System (LSITs) of VIS at eu-LISA's Strasbourg premises, focusing on new functionalities and overall infrastructure security. The report is expected in 2025. In parallel, a follow up audit assessed the implementation of the EDPS recommendations from the 2023 audit for the LSITs of VIS, SIS and Eurodac as well as one for the Internal Market Information (IMI) system managed by the EC's Directorate-General for Internal Market, Industry, Entrepreneurships and SMEs (DG GROW).

As a member of the EDPB, the EDPS, collaborates with the DPAs through the [Coordinated Supervision Committee](#), to strengthen supervision in the AFSJ field.

## Cooperation with the DPO Network

To bridge the gap between data protection law—in particular EUDPR—and its practical application, the EDPS fosters collaboration with the Data Protection Officers (DPOs) of across all EUIBAs, forming the DPO network. The role of DPOs has grown increasingly important (for information on the EDPS DPO' activities please see [dedicated section](#)), especially with the adoption of the GDPR and EUDPR. Leveraging their expertise, DPOs provide independent, tailored advice while addressing their organisations' needs.

---

<sup>40</sup> [EUROSUR](#) is a framework for information exchange and cooperation between Member States and Frontex to improve situational awareness and increase reaction capability at the external borders. EUROSUR includes situational pictures, which contain information on the situation at the borders of a Member State (national situational picture), at the EU external borders (the European situational picture) or on specific operations at the borders (specific situational pictures). It also includes the EUROSUR fusion services, which are satellites and other surveillance tools in the maritime domain and air borders areas.

<sup>41</sup> Namely Frontex, Europol and eu-LISA.

<sup>42</sup> Article 56(2) of the Regulation (EU) 2018/1861 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1861> & Article 70(2) of the Regulation (EU) 2018/1862 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1862>



The EDPS holds two annual DPO network meetings (June and November in 2024), featuring keynotes, updates on EDPS activities, case law presentations, and exchanges of views. A DPO Support Group (6-10 members) helps<sup>43</sup> shape the agenda, prepares workshops, and moderates discussions.

Additionally, EDPS supervisory units meet six DPOs representatives two to three times a year, in roundtables to discuss key topics; summaries of the discussions are then shared across the network. Regular bilateral meetings also continue with the DPOs of the EC, the EP and the Council of the EU.

To enhance communication, an EDPS Contact Point for the DPO Network was established in 2023. The EDPS also provides resources such as 'Quick News for DPO', a hotline, and training for new DPOs.

## Data Breach Notification Management

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to transmitted, stored or processed personal data of individuals. The impact of a personal data breach can be far-reaching, such as identity theft or damage of an individual's reputation. Under EUDPR, all EUIBAs have a duty to report personal data breaches to the EDPS, unless a risk to the affected individuals is unlikely. During 2024, the EDPS continued to monitor and supervise the EUIBAs on their procedures related to personal data breaches<sup>44</sup>.

**125 personal data breach notifications** were received in 2024, out of which 109 admissible and 16 inadmissible. This represents a nearly **40% increase** compared to 2023 (90 personal data breach notifications out of which 77 admissible and 13 inadmissible). Four of them were assessed as posing unlikely risks for data subjects while 12 were submitted by non-EUIBAs.

Out of the 125 personal data breach notifications, 53 were received in phases. These kind of notifications—in phases—are complex incidents requiring multiple actions and exchanges with the controller. By the end of 2024, some notifications in phases were still pending finalisation by the relevant EUIBAs. In one instance, the EDPS determined that a breach posed a high risk to data subjects, contrary to the EUI's initial assessment. As a result, the EDPS ordered the controller to notify the affected data subjects.

For the first time, the EDPS launched a pre-investigation in 2024, following a 2022 personal data breach involving an EC tool used by several EUIs. Additionally, the EDPS made significant progress in addressing a backlog of past data breach notifications. 117 cases were assessed and closed, supported by improved internal management and resources allocation. To enhance oversight, the EDPS introduced new standards, procedures and methods for managing both past and future personal data breaches notifications. These efforts aim to provide EUIBAs with adequate support while ensuring robust supervisory mechanisms to protect the fundamental rights and freedoms of affected data subjects.

In 2024, the EDPS organised one campaign<sup>45</sup> concerning personal data breaches and a cybersecurity exercise<sup>46</sup> on personal data breaches in collaboration with ENISA:

### a. Personal Data Breach Awareness Campaign

This campaign, which ran from March to October 2024, was carried out in the context of the institution's 20th anniversary. This initiative targeted EUIBAs that had not yet reported breaches, aiming to enhance compliance with the EUDPR. The campaign using a four-phase approach, ie. surveys, data analysis, bilateral meetings, and a final report. It emphasised three pillars of breach management: foundational, operational, and improvement capabilities. Key challenges revealed were limited resources, unclear processor roles, and

---

<sup>43</sup> A call for expression of interest is launched at the beginning of each year.

<sup>44</sup> Keeping of registry, assessment of the risk, notification to the EDPS, communication to data subjects, etc.

<sup>45</sup> EDPS' Campaign on raising awareness of personal data breaches: [https://www.edps.europa.eu/data-protection/our-work/publications/reports/2024-12-11-edps-campaign-raising-awareness-personal-data-breaches\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/reports/2024-12-11-edps-campaign-raising-awareness-personal-data-breaches_en)

<sup>46</sup> PATRICIA exercise: [https://www.edps.europa.eu/data-protection/our-work/publications/reports/2024-12-12-patricia-exercise-2024-personal-data-breach-awareness-cybersecurity-incident-handling\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/reports/2024-12-12-patricia-exercise-2024-personal-data-breach-awareness-cybersecurity-incident-handling_en)

insufficient risk management and awareness efforts. Tailored recommendations encouraged increased training, better resource allocation, and risk management frameworks to improve data protection compliance. The campaign concluded with actionable insights and proposed measures to foster continuous improvement in personal data breach management across EUIBAs.

#### b. PATRICIA - Cybersecurity Exercise

In October 2024 the EDPS and the European Union Agency for Cybersecurity (ENISA) jointly organised a table-top exercise titled “Personal dATa bReach awareness In Cybersecurity Incident hAndling” (PATRICIA), at the EDPS premises in Brussels. The exercise aimed to raise awareness among staff from EUIBAs on effective management of personal data breaches.

PATRICIA, developed under the EDPS-ENISA Memorandum of Understanding (MoU), brought together 21 participants from six EUIBAs, including IT managers, DPOs, and Security Officers (LISO, LCO), all of whom play key roles in managing cyber incidents involving personal data breaches. CERT-EU also participated as an observer, sharing valuable insights. The exercise revealed areas for improvement, highlighting the need for a common understanding of responsibilities and interdisciplinary cooperation.

Based on these findings, the EDPS and ENISA provided participants with a recommendations report. Participants praised the exercise, suggesting future editions include more EUIBAs and additional elements on personal data breach management.

By addressing identified issues, EUIBAs can improve their readiness, reduce risks and comply with EUDPR. This exercise demonstrated how the EDPS, in collaboration with ENISA, can support institutions in building capacity, fostering collaboration, and promoting continuous improvement in personal data breaches management.

## Advisory tasks

The EDPS provides guidance on proposed legislation from the EC, which holds the right of legislative initiative, as well as to the EP and the Council of the EU, 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 protection<sup>47</sup>.
- Formal comments: similar to 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 protection<sup>48</sup>.
- 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 opinion<sup>49</sup>.

---

<sup>47</sup> 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.

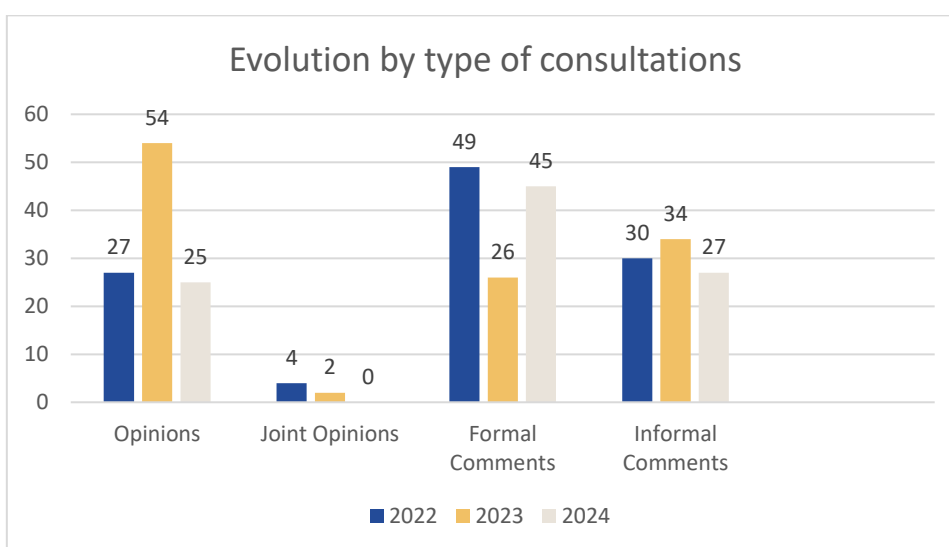
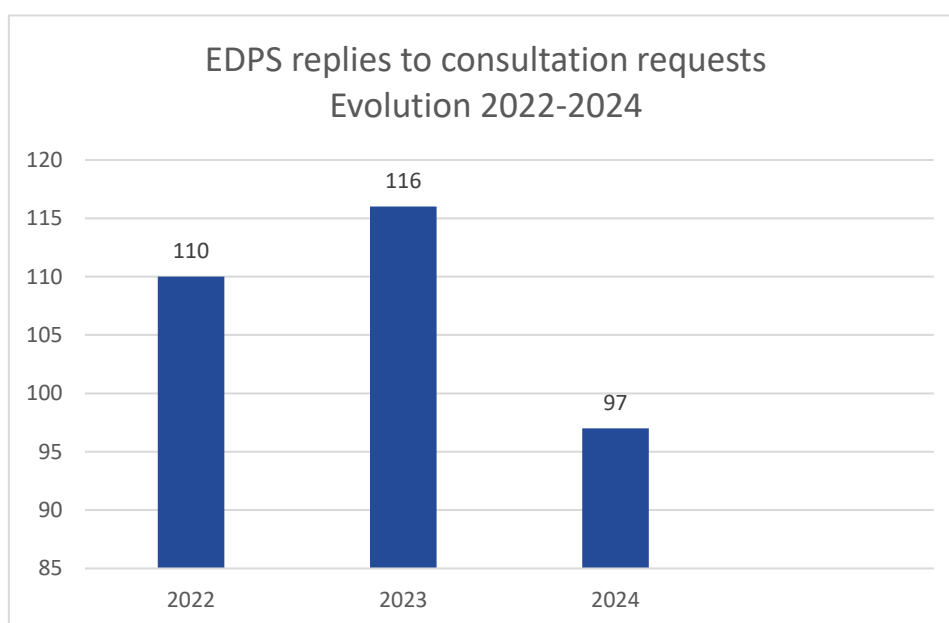
<sup>48</sup> Article 42(1) of EUDPR. Formal Comments are published on the EDPS website.

<sup>49</sup> EDPS' Rules of Procedure: [https://www.edps.europa.eu/about/office-edps/edps-rules-procedure\\_en](https://www.edps.europa.eu/about/office-edps/edps-rules-procedure_en)

## 1. Legislative consultations

Despite being the final year of the previous Commission's mandate and an election year for the European Parliament, the number of legislative consultation requests remained high in 2024. The statistics also reflect the ongoing expectation that the EDPS should be involved and provide advice during the informal stage of legislative and/or policy proposal preparation.

In 2024, the EDPS responded to **97 legislative consultations**, including 70 under Article 42(1); EDPS issued 25 opinions and 45 formal comments. Additionally, it provided 27 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.





## 2. Other advisory activities

Growing awareness of data protection issues has led to increasing requests from EP and its committees<sup>50</sup> and/or individual (shadow) rapporteurs for comments or opinions on compromise amendments on trilogue negotiations. Similarly, invitations from Council working parties to present EDPS opinions have become more frequent. The Supervisor and EDPS staff regularly respond to these requests. The slight increase in staffing since 2018 in combination with sharp rise in consultation requests has also contributed to a decline in the number of EDPS own-initiative opinions.

To address the increasing regulatory complexity introduced by the EU's new 'Digital Rulebook', the EDPS launched 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 effort, the EDPS hosted a seminar on 24 October 2024, to discuss the concept note "Towards a Digital Clearinghouse 2.0". The event aimed to foster debate on digital governance and enforcement, promoting cross-regulatory and addressing the current governance fragmentation, both at EU and national level.<sup>51</sup>

## Advocacy and Cooperation

The EDPS is a key player and respected voice in privacy and data protection discussions. Beyond organising the IPEN event for privacy engineers and monitoring technology projects that contribute to foresight debates within the EUIBAs, EDPS management and senior staff actively participate in policy-making events.

In 2024, the EDPS and its Secretary-General spoke at major events, including the Computers, Privacy and Data Protection (CPDP) conference in Brussels, the Privacy Symposium Conference in Venice, ENISA's Annual Privacy Forum in Lyon, the IAPP Global Privacy Summit in Washington, the First Privacy Symposium in Japan, and the EDEN Conference in Madrid.

Additionally, the EDPS organised and moderated a panel in the event "Data Spaces in EU: Synergies between data protection and data spaces, EU challenges and the experiences of Spain" co-organised by the Spanish DPA and ENISA.

### The EDPS as a member of the European Data Protection Board

While the EDPS is providing the Secretariat of the EDPB acting under the responsibility of the EDPB Chair, the EDPS is also 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 supervisor of EUIBAs. This ensures that EDPB considerations are anchored in Union law, including case law of the Court of Justice of the EU, and underpinned by 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. The EDPS led a taskforce on cooperation with competition and consumer protection authorities, which, amongst other initiatives, is developing joint guidance with the EC on the interplay between the Digital Markets Act (DMA) and the GDPR. In recognition of the importance of the work carried out, the EDPB recently decided to transform this taskforce into a new expert subgroup on cross-regulatory interplay and cooperation, which the EDPS will help coordinate in 2025.

---

<sup>50</sup> LIBE, IMCO, ECON

<sup>51</sup> Towards a Digital Clearinghouse 2.0: <https://20years.edps.europa.eu/en/initiatives/towards-digital-clearinghouse-20>

As a member of the EDPB, the EDPS made significant contributions to various EDPB initiatives in 2024, including:

- the Guidelines on legitimate interest,
- the EDPB Strategy for the years 2024-2027,
- the EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.
- the EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models
- the Guidelines on Article 48 of the GDPR,
- the Statement on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement;
- the EDPB response to the European Commission on Article 15 DMA Consumer Profiling Reports
- the Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR. The Statement is a follow-up to the EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679;
- the EDPB report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework,
- the Guidelines 01/2023 on Article 37 Law Enforcement Directive, adopted on 19 June 2024;
- the Statement on the financial data access and payments package.

## Cooperation with other EUIBAs and participation in Regulatory Boards

### 1. High-level Group for the Digital Markets Act

As a member of the High Level Group (HLG) established under Article 40 of the DMA, the EDPS together with the EDPB has participated in the two first meetings of the HLG. The DMA tasks HLG members to provide the EC with advice and expertise in the areas falling within the competences of its members, including with a view of promoting a consistent regulatory approach across different regulatory instruments, including the GDPR and the ePrivacy Directive. In May 2024, the HLG issued a public statement on Artificial Intelligence.<sup>52</sup>

### 2. European Data Innovation Board

Both the EDPS and EDPB are members of the European Data Innovation Board (EDIB), an expert group established under Article 29 of the Data Governance Act<sup>53</sup> (DGA) and chaired by the EC. The tasks of the EDIB include advising and assisting the European Commission on:

- developing a consistent practice for data altruism and for the registration of data intermediation services and data altruism organisations;

---

<sup>52</sup> Public Statement on Artificial Intelligence: [https://digital-markets-act.ec.europa.eu/high-level-group-digital-markets-act-public-statement-artificial-intelligence-2024-05-22\\_en#:~:text=Personal%20data%20must%20be%20collected,data%20and%20other%20fundamental%20rights](https://digital-markets-act.ec.europa.eu/high-level-group-digital-markets-act-public-statement-artificial-intelligence-2024-05-22_en#:~:text=Personal%20data%20must%20be%20collected,data%20and%20other%20fundamental%20rights)

<sup>53</sup> <https://www.european-data-governance-act.com/>

- 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.

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

The EDPS participated as observer in the HLG on Access to Data for Effective Law Enforcement, jointly established by the Presidency of the Council and the European Commission 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, structured as “Capacity Building measures”, “Cooperation with Industry and Standardisation” and “Legislative measures”.

### 4. Inter-institutional Committee for Digital Transformation (ICDT)

The work of the ICDT is structured into various subgroups, which may further divide tasks into dedicated taskforces. The ICDT Plenary, composed of high-level IT managers from all EUIBAs, meets quarterly to develop common approaches and oversee the work of its subgroups. The EDPS attends plenary meetings and other meetings only on an ad-hoc basis, depending on its interests.

Beyond facilitating coordination among IT managers of EU Institutions, 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.

### 5. Inter-institutional Cybersecurity Board (IICB)

The EDPS is an IICB member, 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 for the IICB, with support from the EDPS Local Information Security Officer (LISO) and Local Cybersecurity Officer (LCO).

### International cooperation

As data flow across borders, data protection should be considered in a global context. In 2024, 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:

## 1. Global Privacy Assembly (GPA)

The EDPS is an active member of the GPA<sup>54</sup> and was the host of the 2018 Conference, which brought together over 1 000 delegates to discuss digital ethics and the challenges of a data-driven society.

The EDPS, jointly with the French data protection authority (CNIL), co-chairs the GPA's working group on Ethics and Data Protection in Artificial Intelligence (AIWG). Additionally, the EDPS participates in other GPA working groups<sup>55</sup>. The 46th GPA conference took place from 28 October to 1 November 2024 in Jersey, hosted by the Personal Data Protection of Jersey, and brought together GPA members and observers from around the world to address key data protection challenges. The outcome of the conference was the adoption of several resolutions on important topics<sup>56</sup>. Notably, the EDPS, along with the Federal Data Protection Commissioner (BfDI) of Germany, presented a resolution on Data Free Flow with Trust (DFFT) as the main sponsor.

During the closed session, the EDPS presented the report of the AI and ethics WG, jointly with the CNIL, and reported on the activities of the Council of Europe, as EDPS represents the GPA as observer to the Committee of Convention 108 (T-PD).

## 2. Council of Europe (CoE)

The EDPS, through its Strasbourg antenna, actively supports the EU's position at the Council of Europe (CoE). It follows the activities of the Consultative Committee of the Convention 108 (T-PD), represents the GPA before the T-PD, and participates as an observer to uphold high data protection standards aligned with EU regulations.

The T-PD activities concern topics of strategic importance for the EDPS such as facial recognition, artificial intelligence (AI), intelligence oversight, digital identity, political data processing including elections, trans-border data flows, inter-state data exchanges on anti-money laundering/countering financing of terrorism and tax purposes, data protection and neurosciences or the use of Privacy enhancing technologies (PET) with regard to the processing of synthetic data and large language models (LLMs). The modernised<sup>57</sup> Convention 108<sup>58</sup>, introduced a crucial follow-up mechanism, through seven ratifications are still needed for its entry into force.

Additionally, the EDPS participated to meetings of the Committee on AI (CAI)<sup>59</sup>, tasked by the Committee of Ministers of the CoE to elaborate a Convention on the development, design, and application of AI systems. CAI developed the Framework Convention on AI and human rights, democracy and the rule of law, the first-ever international legally binding treaty in this field<sup>60</sup>.

## 3. Organisation for Economic Co-operation and Development (OECD)

The OECD's work on data governance and privacy is increasingly relevant to the EDPS. The Working Party on Data Governance and Privacy in the Digital Economy<sup>61</sup> (DGP), reporting to the OECD Committee on Digital Economy Policy (CDEP), develops evidence-based policies in this field. It is composed of delegates from the 38 OECD member countries, including governments and data protection authorities' representatives. The

---

<sup>54</sup> Global Privacy Assembly: <https://globalprivacyassembly.org/> previously known as the International Conference of Data Protection and Privacy Commissioners, ICDPPC.

<sup>55</sup> Global Frameworks and Standards, Digital Economy & Society, Data Protection and Other Rights Freedoms, International Enforcement Cooperation, Digital Citizen and Consumer, The Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management, Data Sharing.

<sup>56</sup> Adopted Resolutions: <https://globalprivacyassembly.org/document-archive/adopted-resolutions/>

<sup>57</sup> Modernisation of Convention 108: <https://www.coe.int/en/web/data-protection/convention108/modernised>

<sup>58</sup> Details of Treaty No. 108: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>

<sup>59</sup> Committee on Artificial Intelligence: <https://www.coe.int/en/web/artificial-intelligence/cai>

<sup>60</sup> EDPS Statement: [https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-statement-view-10th-and-last-plenary-meeting-committee-artificial-intelligence-cai-council-europe-drafting-framework-convention-artificial\\_en](https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-statement-view-10th-and-last-plenary-meeting-committee-artificial-intelligence-cai-council-europe-drafting-framework-convention-artificial_en)

<sup>61</sup> Privacy and Data Protection: <https://www.oecd.org/digital/ieconomy/information-security-and-privacy.htm>

DGP addresses key issues such as Data Free Flow with Trust (DFFT), government access to private-sector data, enforcement cooperation, and Privacy Enhancing Technologies. The EDPS follows DGP activities closely and participates in the Privacy Guidelines Expert Group and the Working Party on AI Governance (AIGO).

Additionally, in line with its priority to promote DFFT, the OECD has formed an expert community to foster trust in its use across borders, bringing together stakeholders from governments, academia, civil society, business, and international organisations to provide project-based technical perspectives and evidence to the policy-oriented work of the Digital Policy Committee (DPC) of the OECD and its Working Party on Data Governance and Privacy (WPDGP). The EDPS has been invited to join this Expert Community and will take part in the ongoing activities of this group.

#### 4. Cooperation with international organisations

On 23 - 24 September 2024, the EDPS co-organised the International Organisations Workshop on data protection (IOW)<sup>62</sup>, with the World Bank, in Washington, D.C - the first edition held outside Europe. This marked a step towards strengthening its global reach and promoting data protection principles worldwide.

Since its creation, IOW<sup>63</sup> has served as a platform for international organisations to discuss pressing data protection issues and share best practices. Each year, the EDPS co-hosts the workshop in collaboration with a different organisation.

In 2024, coinciding with the EDPS's 20th anniversary, a high-level panel reflected on the workshop's evolution and achievements over the past two decades, and future direction. A dedicated AI panel examined both the potential of AI and its data protection challenges, emphasising the need for sharing best practices to balance innovation and privacy.

The workshop also featured two practical sessions: one on managing personal data breaches and another on ensuring IT tools meet high privacy standards. Additionally, two breakout sessions fostered discussions, one on data transfers involving international organisations and another on challenges faced by data protection officers. These sessions encouraged deeper engagement and knowledge exchange among participants.

#### 5. G7 Data Protection Authorities (DPAs) roundtable

From 9 to 11 October 2024, the EDPS attended the G7 DPAs Roundtable in Rome, Italy, hosted by the Italian data protection authority (Garante). This annual event brought together representatives from Canada, France, Germany, Japan, the United Kingdom, and the United States, with the EDPB and the EDPS jointly representing the EU.

Discussions focused on three core areas: Data Free Flow with Trust (DFFT), emerging technologies, and enforcement cooperation. A major outcome was the adoption of a statement<sup>64</sup> on the role of DPAs in fostering trustworthy AI, emphasising their crucial role in ensuring responsible AI use.

Additionally, the DPAs issued a "Statement on AI and Children" urging action to safeguard children's privacy and ensure AI fosters trust while protecting the most vulnerable.

The G7 DPAs also adopted:

---

<sup>62</sup> Workshop on Data Protection 2024: [https://www.edps.europa.eu/data-protection/our-work/publications/events/2024-09-23-international-organisations-workshop-data-protection-2024\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/events/2024-09-23-international-organisations-workshop-data-protection-2024_en)

<sup>63</sup> Data Protection and International Organisations: [https://www.edps.europa.eu/data-protection/our-work/international-cooperation/data-protection-and-international-organisations\\_en](https://www.edps.europa.eu/data-protection/our-work/international-cooperation/data-protection-and-international-organisations_en)

<sup>64</sup> [https://www.edps.europa.eu/system/files/2024-10/draft\\_statement\\_dpas\\_governance\\_trustworthy\\_ai\\_en.pdf](https://www.edps.europa.eu/system/files/2024-10/draft_statement_dpas_governance_trustworthy_ai_en.pdf)

- a comparative analysis of the EU GDPR certification as the Global Cross-Border Privacy Rules (CBPR) System in a controller-to-controller scenario;
- a terminology paper on anonymisation, pseudonymisation, and de-identification;
- a narrative on 'Promoting Enforcement Cooperation';
- a G7 DPAs Communiqué and the 2024/2025 G7 DPAs Action Plan.

## 6. Spring Conference

The EU DPAs and the Council of Europe hold an annual Spring Conference to discuss common interests, emergent trends, and developments in privacy and data protection. The event fosters cooperation between Europe's data protection systems and professionals while facilitating the exchange of best practices.

A delegation from the EDPS attended the 32nd European Conference of Data Protection Authorities, held in Riga, Latvia on 13-16 May 2024. During the conference, DPAs adopted a resolution on enhanced cooperation, reaffirming their commitment to work together to address the challenges and opportunities of borderless nature of data processing.

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

On 12 September 2024, EDPS participated in the event "Data protection in the Western Balkans and Eastern Partnership Region", organised by SIGMA Programme, the Eastern Partnership Regional Fund for Public Administration, the Regional Cooperation Council and the Regional School of Public Administration.

Bringing together DPAs and public institutions from 11 countries<sup>65</sup>, the event facilitated discussions on challenges and opportunities in advocating for digital rights and privacy protection.

The EDPS insisted on the importance of continued and strong international cooperation, conducive to elevating data protection standards according to shared values and rights. The EDPS Secretary-General presented the EDPS' strategy on AI, detailing current actions to face challenges as well as opportunities that AI systems may bring. As the EUIBAs' data protection authority, the EDPS aims to ensure that AI is developed in a human-centric and sustainable way, respecting privacy and data protection principles.

During the biggest part of the meeting more technical and practical data protection matters on a wider range of topics of common interest were discussed, such as:

- the GDPR's interplay with new European regulations (Digital Services Act, Digital Markets Act, Data Governance Act, and the Data Act);
- investigation policies and methodologies;
- the Council of Europe's legal framework and cooperation activities on data protection;
- the regulation on global data flows, biometrics, and facial recognition.

## 8. International Working Group on Data Protection in Technology (IWGDPT, also known as Berlin Group)

In November 2024, the EDPS co-hosted the 74th meeting of the IWGDPT as part of its 20th-anniversary celebrations efforts to strengthen international cooperation in technology monitoring and foresight. The IWGDPT brings together representatives from global data protection authorities and independent experts

---

<sup>65</sup> Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Kosovo, Moldova, Montenegro, North-Macedonia, Serbia and Ukraine.



from public and private sectors, academia, and civil society. The group regularly discusses privacy challenges and publishes guidance documents that help shape international data protection policies in technology.

Held at the European Parliament's Visitor Centre, the 74th meeting saw a record participation and received high praise for its organisation, which included a social dinner and a visit to the House of European History.

Discussions focused on technological developments across jurisdictions, draft papers, and future research topics. Feedback confirmed the event's success in reinforcing the EDPS's role in technology monitoring and global data protection cooperation.

## Cybersecurity Cooperation

### 1. Memorandum of understanding with the European Union Agency for Cybersecurity (ENISA)

The EDPS has undertaken several initiatives under the 2023-2025 Strategic Action Plan of its Memorandum of understanding (MoU) with ENISA. The MoU fosters joint efforts on cybersecurity in data protection, securing personal data in cybersecurity operations, and promoting privacy enhancing technologies. Key actions, include support for 2024 Annual Privacy Forum 2024, participation in the joint PATRICIA cybersecurity exercise (more info see [here](#)), and involvement in Cyber Europe 2024. The EDPS views the MoU with ENISA as a strategic pillar for effective data protection supervision within EUIBAs.

### 2. Cyber Europe 2024

The EDPS participated in the Cyber Europe 2024, a cybersecurity exercise, organised by ENISA, simulating large-scale cyber incidents in the EU energy sector. The event involved over 1 000 participants from 30 countries, tackling challenges such as Distributed Denial-of-Service (DDoS) attacks, energy supply chain disruptions, and cyberattacks on industrial systems. A data breach scenario was also analysed to refine response strategies. The EDPS's involvement strengthened collaboration with ENISA, enhanced staff expertise in cybersecurity and data protection, and supported a joint approach to tackling cyber threats while identifying areas for improvement.

## Technology monitoring tasks

Technology Monitoring is an increasingly vital task of the EDPS, mandated under Art. 57(h) of the EUDPR. It enables the EDPS to assess the impact of technological developments on data protection and anticipate future through foresight analysis. In 2024, the EDPS strengthened its technological assessment capabilities and digital innovation capacity while maintaining active engagement with the public and privacy experts.

### 1. TechDispatches

In 2024, the EDPS, in collaboration with the Spanish data protect authority (AEPD), published a TechDispatch on Neurodata<sup>66</sup>. While neurodata processing is not new, recent advancements have enabled new—and often concerning—use cases.

---

<sup>66</sup> Neurodata: [https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en)

This TechDispatch explores how different types of neurodata processing facilitate various applications, both present and future. It also highlights potential risks, emphasising how certain uses of neurodata can seriously impact fundamental rights, freedoms, and human dignity.

## 2. TechSonar

In November 2024, the EDPS published its 4<sup>th</sup> issue of its TechSonar initiative, which explores emerging technologies and their impact on data protection and strategic foresight. TechSonar is the first European initiative to bridge data protection with forecasting, foresight, and future studies, addressing upcoming technological challenges.

This edition took a new approach, to showcasing the latest technologies, reflecting the EU's AI Act, which came into effect in 2024, and the EDPS's role as the leading AI authority for EUIBAs. With AI adoption accelerating, the report focuses on key AI trends shaping 2024, such as LLMs and Federated Learning.

The 2025 TechSonar report<sup>67</sup> explores six emerging AI-related technologies:

- Retrieval-augmented generation (RAG),
- On-device AI,
- Machine unlearning,
- Multimodal AI,
- Scalable oversight, and
- Neuro-symbolic AI.

Each of these trends begins with a fictional scenario illustrating a potential real-world application, followed by a description of the technology, its current development status, and its impact on individuals. The report concludes with recommended reading for deeper exploration.

## 3. Internet Privacy Engineering Network (IPEN)

Founded by the EDPS in 2014, the IPEN initiative promotes privacy engineering and advances best practices in the field. Since then, the EDPS organises yearly IPEN events or workshops, often in connection with the ENISA Annual Privacy Forum.

For 2024, the chosen theme was “Human oversight of automated decision-making”. While regulations require human oversight to ensure AI-driven decisions remain accountable, the concept itself remains vague and complex. Experts continue to debate what effective oversight entails and how to implement it in practice.

In September 2024, the EDPS and Karlstad University co-hosted an IPEN event<sup>68</sup> to examine the purpose, capacities, and limitations of human oversight in automated decision-making. Privacy experts and researchers discussed expectations and requirements for ensuring meaningful oversight of automated systems.

The next IPEN event is scheduled for October 2025 in Frankfurt, Germany.

## 4. Actions with the Memorandum of Understanding with the Spanish Data Protection Authority (AEPD)

The EDPS has undertaken two key actions under its MoU with the 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.

---

<sup>67</sup> TechSonar Report 2024: [https://www.edps.europa.eu/data-protection/our-work/publications/reports/2024-11-15-techsonar-report-2025\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/reports/2024-11-15-techsonar-report-2025_en).

<sup>68</sup> IPEN event on “Human oversight of automated decision-making”: [https://www.edps.europa.eu/data-protection/technology-monitoring/ipen/ipen-event-human-oversight-automated-making\\_en](https://www.edps.europa.eu/data-protection/technology-monitoring/ipen/ipen-event-human-oversight-automated-making_en)



In line with the MoU commitments, the AEPD and EDPS jointly supported research, studies, and reports on data protection. In June 2024, they published a TechDipatch on Neurodata<sup>69</sup> and are currently preparing a second TechDipatch on Federated Learning, set for release in early 2025.

## 5. Website Audits

In August 2024, the EDPS sent 17 reports to 13 EUIBAs, concluding the second and final wave of remote website audits. These reports assess compliance with EUDPR, focusing on:

- website security and safeguards
- use of trackers during browsing
- clarity and adequacy of information provided to users

The audits evaluate how these websites handle personal data processing and ensure adherence to data protection standards.

## 6. Website Compliance Awareness Campaign (WCAC)

EUIBAs manage more than 1 300 websites, making individual audits impractical given EDPS' limited resources. To improve compliance efficiently, the EDPS launched the WCAC, for raising awareness on potential compliance issues, under Article 57(1) (c) EUDPR. This initiative helps controllers to meet their accountability obligations under Article 4(2) EUDPR.

In 2018, the EDPS developed the Website Evidence Collector (WEC) tool for its remote website audits. This tool was made publicly available so that controllers and DPOs could identify potential issues and areas of improvement on their websites. Despite the WEC's availability, its knowledge and use by EUIBAs remains limited. In the pilot phase of this campaign, the EDPS will employ the WEC to regular check (every 6 months) one EUIBA website out of the existing 76.

The WEC output will be fine-tuned to produce a factual, simplified report per website. These reports will help DPOs and controllers to identify and assess data protection weaknesses—particularly Article 37 EUDPR, and Article 5(3) Directive 2002/58/EC ('ePrivacy Directive')—and take corrective actions if needed.

This pilot project of website scans will be carried out in three waves: first one in autumn 2024, a second one in spring 2025 and a third one in autumn 2025. After each wave, each EUIBA receives a notification including the report with the results of the WEC tool execution, information about next steps of the pilot and a reminder of the option to use the WEC tool proactively. The inclusion of a website in this campaign does not preclude the EDPS to make use of its supervisory actions, including investigation of this website.

At the end of the WCAC pilot phase (autumn 2025), the EDPS may use the collected information as a risk indicator to identify EUIBAs responsible for specific websites for potential review through investigation or audit. If the pilot proves successful and resources allow, the EDPS will consider expanding the campaign to cover all 1 300+ websites under EUIBAs' responsibility.

## Data Protection Activities

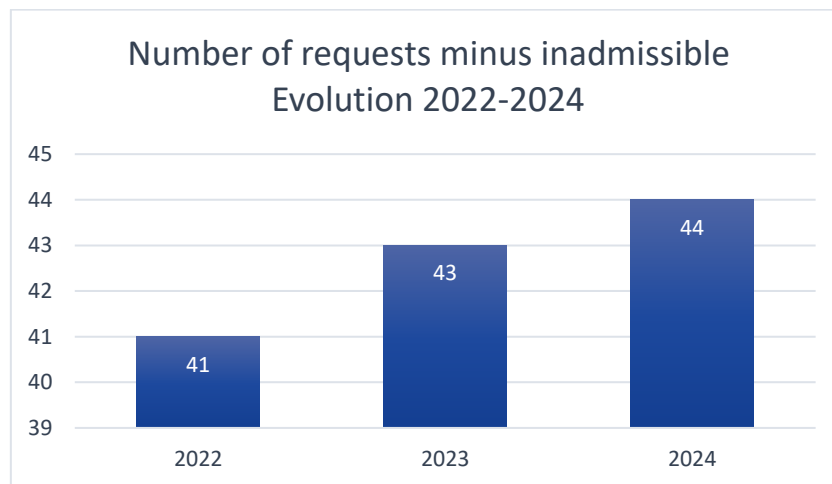
In 2024, the Data Protection Officer (DPO) collaborated with delegated controllers to strengthen EDPS' data protection compliance and accountability.

---

<sup>69</sup> [https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en)

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 2024, the DPO processed 44 data subjects' requests<sup>70</sup> (excluding inadmissible requests). In certain cases, individuals exercised more than one data protection right, such as access and information requests.



The DPO also assisted in handling 16 personal data breaches. Due to the low risk to natural persons' rights and freedoms, 15 did not require notification to the supervisory authority (SA), while one was reported and mitigated accordingly.

In 2024, 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 June 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 documents<sup>71</sup>. For each request submitted to the EDPS, the Transparency officer collaborates with the relevant services for responding appropriately to the request.

In 2024, the EDPS received 53 access to documents requests, out of which five<sup>72</sup>, were confirmatory applications (appeals). In seven cases access to the documents falling within the scope of the request were

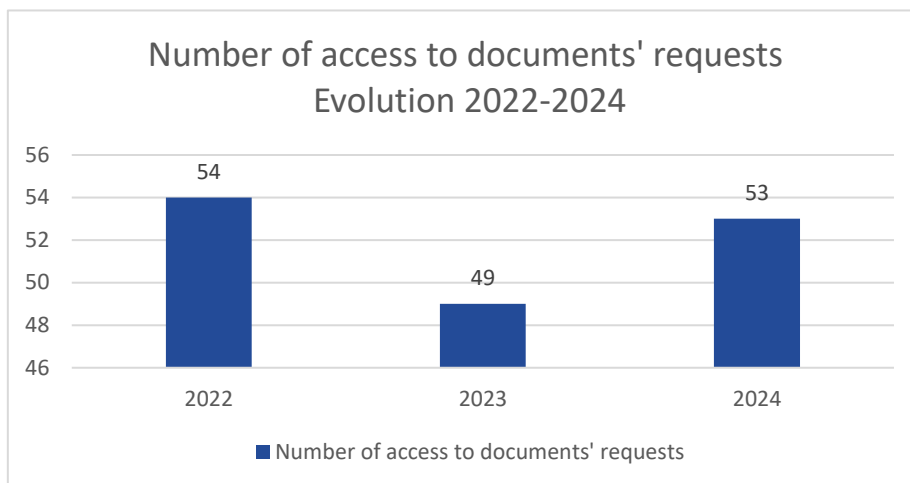
<sup>70</sup> More specifically, the EDPS replied to 19 access requests, 13 erasure requests, six information requests, one rectification request, two objection requests, three consent withdrawals and 47 inadmissible requests.

<sup>71</sup> 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>

<sup>72</sup> Representing ~10% of all cases in 2024.

denied as they were covered by exceptions<sup>73</sup>. In all other cases where documents could be identified, they were either fully or partially disclosed to the applicant.

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

Transparency is a core value, ensuring clear and accessible communication about our work and objectives. To achieve this, the EDPS has built a strong online presence through its website and social media channels using tailored communication tools to engage different audiences and enhance visibility.

Key communication platforms include:

- @EU\_EDPS X account<sup>74</sup> showcasing EDPS participation in events and highlighting key messages.
- European Data Protection Supervisor LinkedIn account<sup>75</sup> engaging with privacy and data protection professionals, making it the fastest-growing platform with the most active followers.
- Newly-opened Instagram @eu\_edps account<sup>76</sup> (launched in February 2024) sharing educational, informative and engaging content.
- YouTube channel<sup>77</sup> hosting event footage, awareness-raising videos and Supervisor's speeches, including the 20 Talks video series and 20th anniversary summit.

Successful campaigns across these platforms include:

- #InCaseYouMissedIt : raising awareness of overlooked topics and past activities.
- Blue Book: promotion via short videos
- Cybersecurity awareness: playful, engaging content on cyberattacks, AI and data breaches.

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

<sup>74</sup> EDPS' X account: [https://x.com/EU\\_EDPS?ref\\_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor](https://x.com/EU_EDPS?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor)

<sup>75</sup> EDPS' LinkedIn account: <https://www.linkedin.com/company/edps/?originalSubdomain=be>

<sup>76</sup> EDPS' Instagram account: [https://www.instagram.com/eu\\_edps/](https://www.instagram.com/eu_edps/)

<sup>77</sup> EDPS' YouTube Channel: <https://www.youtube.com/c/europeandataprotectionsupervisor>

The EDPS website<sup>78</sup> remains the primary communication channel, covering work on supervision, enforcement, policy, consultation, technology, privacy and AI. It also hosts a monthly newsletter and blog posts, featuring personal insights from the Supervisor's and the Secretary General.

Beyond public outreach, media engagement remains strong, with a network of over 300 journalists. In 2024, 12 press releases covered key topics including AI, the investigation into Microsoft tools used by EUIBAs (read more [here](#)) and collaboration with EU data protection authorities.

Events organisation has expanded significantly. Here is a selection of the most outstanding events of the year:

- EDPS Summit<sup>79</sup> marking institution's 20 years of existence, a unique opportunity to gather experts and about the future of data protection.
- CPDP Conference Data Protection Day<sup>80</sup> the first edition, co-organised with the Council of Europe, and CPDP.
- International Organisations Workshop<sup>81</sup> in cooperation with the World Bank in Washington, USA.

In addition to these examples of events, we continued to organise a number of study visits as a way to engage with academic and technology-focused audiences.

Collaborative remains a priority, with active participation in the Inter-institutional Online Communication Committee (IOCC) and joint efforts with other institutions, such as ENISA, the EU's Cybersecurity Agency, for further amplifying the impact of EDPS initiatives.

## Creation of the Artificial Intelligence Unit

Recognising the transformative impact of artificial intelligence (AI), the EDPS established its AI Unit on 1 October 2024, to address new supervisory tasks assigned to the EDPS by the AI Act. This decision reflects our commitment to ensuring that AI systems used by EUIBAs comply with the AI Act, at the same time that they uphold fundamental rights, privacy, and data protection principles.

The Unit operates on three pillars: Governance, risk management, and supervision. Under the AI Act, the EDPS assumes the role of notified body and market surveillance authority, the competent authority for the supervision of AI systems provided, deployed or used by EUIBAs under the AI Act. Tasks in this remit include monitoring compliance, handling complaints, conducting audits, and reviewing Fundamental Rights Impact Assessments.

To facilitate AI governance, the EDPS launched the AI Act Correspondents Network, connecting AI representatives across EUIs to exchange knowledge and align on compliance strategies. This network follows the model of the existing DPO network.

Since its launch, the AI Unit has actively participated in the AI Board and its subgroups, shaping the implementation of the AI Act alongside Member States. It collaborates with the EC's AI Office and other EUIBAs to ensure consistent AI oversight.

To strengthen EDPS expertise, the organisation invested in specialist recruitment and training, including AI risk management courses and international cooperation with the OECD and the Council of Europe. Through

---

<sup>78</sup> EDPS' website: <https://www.edps.europa.eu/en>

<sup>79</sup> EDPS Summit: <https://20years.edps.europa.eu/en/summit/about-summit.html>

<sup>80</sup> CPDP Conference Data Protection Day: [https://www.edps.europa.eu/data-protection/our-work/publications/events/2024-01-25-cpdp-data-protection-day\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/events/2024-01-25-cpdp-data-protection-day_en)

<sup>81</sup> International Organisations Workshop: [https://www.edps.europa.eu/data-protection/our-work/publications/events/2024-09-23-international-organisations-workshop-data-protection-2024\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/events/2024-09-23-international-organisations-workshop-data-protection-2024_en)

these efforts, the AI Unit aims to build a transparent AI governance framework that safeguards the market and the rights of consumers, while fostering innovation in EUIBAs. The EDPS is therefore thoroughly preparing for the new roles and powers under the AI Act.

## Secretariat of the European Data Protection Board

The Secretariat of the European Data Protection Board<sup>82</sup> (EDPB Sec) 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). Staff at the EDPB Sec 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 a Memorandum of Understanding<sup>83</sup>. The EDPB Sec consists of 39 staff members. In addition, seven staff members work within the EDPS for the support provided to the EDPB Sec via horizontal administrative services.

The EDPB budget forms part of the broader EDPS budget. For 2024, the adopted budget of the EDPB amounted to EUR 8.36 m. 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 Sec staff.

### Analytical support to EDPB activities for the year

The EDPB Sec 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 Supervisory Authorities (SAs) across Member States.

#### 1. Binding decisions

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

#### 2. Consistency opinions

DPAs may seek consistency opinions from the EDPB under Art. 64(1) GDPR, addressed to DPAs, including: opinions on draft decisions regarding Binding Corporate Rules (BCRs), 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. Following a consistency opinion, DPAs adopt their national decisions.

In 2024, the EDPB has adopted **28 such consistency opinions**, out of a total of 207 consistency opinions adopted since 2018. For the vast majority of these opinions, the EDPB Sec held the pen. This way, starting from a theoretical description of new compliance tools introduced in the GDPR, the EDPB has built a framework for the new compliance tools, such as codes of conduct and certification mechanisms, to become operational in a consistent manner.

---

<sup>82</sup> European Data Protection Board: [https://www.edpb.europa.eu/about-edpb/who-we-are/edpb-secretariat\\_en](https://www.edpb.europa.eu/about-edpb/who-we-are/edpb-secretariat_en)

<sup>83</sup> Memorandum of Understanding: Signed on 25 May 2018 and available at [https://www.edpb.europa.eu/sites/default/files/files/file1/memorandum\\_of\\_understanding\\_signed\\_en.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/memorandum_of_understanding_signed_en.pdf)

In addition, in 2024, there was a surge in the number of Art. 64(2) consistency opinions. Art. 64(2) GDPR provides a mechanism for the EDPB to issue consistency opinions on matters of general application or those with significant cross-border implications. The Art. 64(2) GDPR framework plays a pivotal role in resolving ambiguities in the GDPR interpretation, especially in areas influenced by emerging technologies or evolving legal contexts. These opinions help avoid conflicting DPA decisions and ensure GDPR rules are applied consistently in the EU. Such opinions can be requested by the EDPB Chair, DPAs, or the Commission.

In 2024, the EDPB adopted Art. 64(2) GDPR opinions on – among others – the following topics: definition of “main establishment” of a data controller, the use of “Consent or Pay” models by large online platforms, the use of facial recognition technologies at airports, obligations of data controllers engaging data processors and sub-processors and ensuring GDPR compliance in AI models.

### 3. 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 DPAs 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.

In 2024, the EDPB adopted two new guidelines, namely guidelines 01/2024 on processing personal data based on legitimate interest and guidelines 02/2024 on processing personal data in response to requests from non-EU public authorities - and updated two guidelines following public consultation.

### 4. Statements on legislative developments

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

In 2024, the EDPB issued the following statements<sup>84</sup>:

- Statement 1/2024 on the Proposal for a Regulation to Prevent and Combat Child Sexual Abuse;
- Statement 2/2024 on the Financial Data Access and Payments Package;
- Statement 3/2024 on data protection authorities’ role in the Artificial Intelligence Act framework;
- Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR.

### 5. 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 Sec has a leading role in implementing and coordinating the following programmes:

- The Support Pool of Experts (SPE)<sup>85</sup>

---

<sup>84</sup> [https://www.edpb.europa.eu/our-work-tools/our-documents/publication-type/statements\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/publication-type/statements_en)

<sup>85</sup> Support Pool of Experts: [https://www.edpb.europa.eu/about-edpb/who-we-are/edpb-secretariat\\_en](https://www.edpb.europa.eu/about-edpb/who-we-are/edpb-secretariat_en)

The 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<sup>86</sup>, provides critical technical expertise and tools to address complex cases and emerging data protection challenges. In 2024, six major projects were undertaken to enhance the GDPR compliance and enforcement across the EU.

One major project involved creating a case digest on Security of Processing and Data Breach Notification<sup>87</sup>. 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 EDPB Website Auditing Tool<sup>88</sup>, which was specifically designed to assist DPAs in evaluating website compliance, including aspects such as cookie management, transparency requirements, and consent mechanisms. The Standardised Messenger Audit<sup>89</sup> project addressed the GDPR compliance challenges in widely used business communication platforms.

The SPE programme also facilitated tailored Data Protection Officer (DPO) training in Croatia<sup>90</sup>. This initiative aimed to equip DPOs with sector-specific expertise to enhance the GDPR compliance, particularly in critical sectors. The AI Risk Assessment project<sup>91</sup> provided tools to address privacy risks in AI systems. For example, it looked at technologies like Optical Character Recognition (OCR), which converts scanned text into readable text, and Named Entity Recognition (NER), which identifies names, organisations, and locations in documents. Complementing this effort, the AI Auditing project<sup>92</sup> developed robust methodologies for auditing AI systems, ensuring their alignment with the GDPR principles such as transparency, fairness, and accountability.

In addition to these initiatives, the EDPB organised a Mobile Apps Bootcamp in September 2024, which built on the success of previous capacity-building events. The bootcamp brought together 50 auditors from 24 countries and the EDPS for a series of expert-led sessions.

- The Memorandum of Cooperation with PEReN

In April 2024, the EDPB signed a Memorandum of Cooperation with PEReN, an interdepartmental office operating under the joint authority of the French Ministers of Economy, Culture, and Digital Technology. This agreement represents a significant milestone in enhancing technical collaboration to address emerging data protection challenges across Europe. The Memorandum formalises a partnership aimed at advancing expertise in critical areas such as mobile application auditing, innovative data science methodologies, and ensuring transparency in algorithmic systems. A particular focus of the cooperation lies in developing advanced tools to support trustworthy artificial intelligence, prioritising the monitoring and auditing of AI systems for GDPR compliance.

- Chat GPT task force

In 2023, the EDPB established the ChatGPT Taskforce, in the absence of a unified enforcement mechanism under the One-Stop-Shop (OSS) framework, as OpenAI had no EU establishment prior to February 2024. The work of the TF continued in 2024 to ensure consistent GDPR application, and tackle the unique risks associated with ChatGPT's processing activities. Key areas of investigation included data accuracy,

---

<sup>86</sup> EDPB Strategy 2024-2027: [https://www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2024-2027\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2024-2027_en)

<sup>87</sup> One-Stop-Shop case digest on Security of Processing and Data Breach Notification: [https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/one-stop-shop-case-digest-security\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/one-stop-shop-case-digest-security_en)

<sup>88</sup> EDPB Website Auditing Tool: [https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/edpb-website-auditing-tool\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/edpb-website-auditing-tool_en)

<sup>89</sup> Standardised Messenger Audit: [https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/standardised-messenger-audit\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/standardised-messenger-audit_en)

<sup>90</sup> Data Protection Officer Training: [https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/data-protection-officer-training\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/data-protection-officer-training_en)

<sup>91</sup> AI Risk Assessment Project: [https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-risks-optical-character-recognition\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-risks-optical-character-recognition_en)

<sup>92</sup> AI Auditing Project: [https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-auditing\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-auditing_en)



transparency, fairness, and compliance with individual rights. Preliminary findings highlighted the necessity of embedding "data protection by design and by default" (DPbDD) into AI systems to mitigate these risks and reinforce accountability for data controllers managing personal data on an unprecedented scale.

- The Coordinated Enforcement Framework (CEF)

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

- The EDPB Secondment programme

In 2024, the programme facilitated an impressive 61 secondments across 27 authorities that will take place in 2024 and 2025, providing participants with invaluable opportunities to deepen their expertise and enhance their operational capabilities. These secondments have not only enabled participants to exchange practical knowledge and insights but have also allowed them to observe different enforcement approaches and best practices in diverse regulatory environments. For many, the experience extended beyond technical learning, fostering professional networks and long-lasting relationships that underpin cooperation among DPAs.

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

## 6. Litigation

In 2024, the EDPB was involved as a party in **13 cases** before the **CJEU**, of which ten were submitted in 2023, one at the end of 2022 and one in 2021. The vast majority of the cases concerned applications for annulment against EDPB binding decisions.

In the context of these proceedings, the EDPB Sec worked closely with external lawyers throughout the different stages of the proceedings, for defining the EDPB's defence strategy and drafting procedural documents. In addition, the EDPB was also involved as an intervener in one case, in support of the EDPS.

## 7. Coordinated Supervision Committee

The Coordinated Supervision Committee (CSC) is a group of national SAs and the EDPS. It ensures coordinated supervision of large scale IT systems and of EU bodies, offices and agencies, in accordance with Article 62 of EUDPR or with the EU legal act establishing the large scale IT system or the EU body, office or agency.

The EDPB Sec 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 2024, the CSC met five times.

In 2024, the activity of the CSC was extended to the supervision of the Visa Information System (VIS), in addition to the Schengen Information System (SIS), Europol, the EPPO, Eurojust and IMI that were already falling under the framework of the EDPB activities.

While the addition of the European Travel Information and Authorisation System (ETIAS) to CSC was postponed to a few months after the start of the Entry and Exit System (EES), which has been further



postponed, substantial work has been dedicated to the preparation of the supervision of ETIAS, with the CSC participating as a member to the ETIAS Fundamental Rights Guidance Board and the creation of a dedicated Working Group on ETIAS.

In the near future, the interoperability will interconnect seven EU-information systems, three existing systems (SIS, VIS, Eurodac and PrümII) and three new systems, yet to be set up (EES, ETIAS and ECRIS-TCN).

The CSC also provides a forum for cooperation in the context of the supervision of the European Public Prosecutor's Office (EPPO), the Custom Information System established under Council Decision 2009/917/JHA and in the context of the supervision of personal data processing activities covered by Regulation (EU) 2023/2854 ("Data Act"), Regulation (EU) 2023/1773 on the carbon border adjustment mechanism transitional registry and Commission Implementing Regulation 2024/3084 establishing an Information System to facilitate the transfer of information between Member States competent authorities, and customs authorities related to deforestation and forest degradation.

## Logistical and administrative support to the EDPB

### International Compliance

#### 1. Data Protection Activities

The EDPB processes personal data according to the rules laid down in EUDPR on the processing of personal data by the EUIBAs. In accordance with Art. 43 of this Regulation, the EDPB has its own DPO team, which is part of the EDPB Sec. In 2024, the EDPB received 18 data subject requests made on the basis of rights enshrined in Art. 17 to Art. 24 of EUDPR. The EDPB Sec also provided assistance with replying to individual requests for information involving the processing of their personal data, and supported in handling six data breaches under Arts. 34 and 35 of EUDPR which required a notification to the EDPS.

#### 2. Access to documents

In accordance with Art. 32 (2) of the EDPB Rules of Procedure (RoP), the EDPB Sec prepares the answers to access requests of EDPB documents which are handled and signed by the Chair or one of the Deputy Chairs. In 2024, the EDPB Sec received 27 public access requests for documents held by the EDPB. Confirmatory applications were received in three cases. No complaint regarding an EDPB confirmatory decision for a request for access to documents was brought to the attention of the European Ombudsman (EO) in 2024.

#### 3. Communication, IT & Administration

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

An important awareness raising action in 2024 for which the EDPB Sec took the lead was the translation of the **Data Protection Guide for Small Business** in 18 languages. This guide aims to provide practical information to SMEs about GDPR compliance in an accessible and easily understandable language. The main goal of the guide is to help raise awareness of the GDPR among SMEs and to facilitate compliance. The development of tools providing practical, easily understandable and accessible data protection guidance is key to reaching a non-expert audience and promoting data protection in practice.

The IMI system is essential for the GDPR cooperation among EDPB members. In 2024, this system facilitated more than 5.644 procedures. There were 907 support requests related to the use of IMI. Overall, the EDPB Sec handled a total of 4.225 support enquiries across all EDPB IT systems.

EDPB HUB, EDPB's primary platform for information sharing with their members, saw significant activity. Over 12 350 different content types were created. This includes, among others, 2 372 new pages, 8 217 documents, 1 389 exchanges. The platform is widely used across various authorities, supporting a substantial user base of over 1 400 members.

The EDPB Sec also ensured the continued usability of the EDPB website which was visited 329 432 times in 2024.

In 2024, the EDPB Sec organised 533 remote, physical and hybrid meetings.

It also processed the translation of 18 EDPB documents in 23 official languages and organised 19 missions for the EDPB Chair.

## **EDPS-EDPB Joint opinions**

No joint opinion was issued in the course of 2024.

# **Resources management**

## **Human resources**

### **Development of employees, teams and of the organisation**

Equipping employees with the right skills directly impacts organisational success. With evolving technologies and new EDPS obligations, such as those under the AI Act, staff require specialised and up-to-date training. To expand learning opportunities, a new policy on online learning platforms was adopted in 2024, with a particular focus on AI literacy. Tailored training courses were offered to EDPS and EDPB staff based on their background and needs.

The EDPS continued its efforts in 2024 with job-shadowing programmes and skill-building initiatives. It joined the new inter-institutional Job Shadowing Programme, pairing staff with colleagues from other EUIBAs to enhance mutual understanding of roles and procedures. Five EDPS staff shadowed European Commission colleagues, while five colleagues from other EUIBAs were welcomed at the EDPS.

Team building activities remained a priority. The EDPS Learning & Development (L&D) coordinator supported team building activities, helping teams strengthen collaboration, define their mission and set priorities. In October 2024, the EDPS/EDPB away day featured compassion break sessions and discussions on key topics. The afternoon session was dedicated to AI preparedness, with high-level speakers and workshops on AI internal use, learning and support tools. In January 2024, EDPS management team attended a leadership development seminar at the Jean Monnet House, co-facilitated by the European School of Administration (EuSA).

Hybrid working prompted EDPS Human Resources and Budget Administration Unit (HRBA) to organise informal events fostering cross-unit interaction, including a clothing swap and Christmas workshops. Two internal calls were launched at the end of 2024:

- Internal facilitators: training staff to lead team events, task forces, and network projects as well as team-building and brainstorming exercises.
- Climate cross-unit Working Group: volunteers working on reducing EDPS/EDPB carbon footprint.

September 2024 marked a key organisational development with the creation of a dedicated AI unit, reassigning four staff members, including an acting Head of Unit. A call for expression of interest was launched to recruit five new staff members as from early 2025. HR processes were further modernised. The mid-term appraisal interviews were replaced with regular informal feedback, fostering a feedback-driven culture. Staff selection procedures were also automated for efficiency.

To strengthen talent retention and attraction, HRBA developed a 'Strategic reflections on talent retention' document outlining short/medium and long-term actions for ensuring a sustainable talent strategy for the EDPS.

## Staff

To address the data protection challenges posed for instance by artificial intelligence (AI), the EDPS seeks to bring together a diverse team of legal and technical experts, as well as specialists from across the EU, to work on shaping data protection. The recruitment processes for both the EDPS and the EDPB are centrally managed by the HRBA. In addition to recruiting data protection experts, the EDPS hires various other profiles to support the institution in its work and manages long and short term replacements. For short term replacements, interim staff is hired.

In 2024, the EDPS conducted 38 selection procedures, with 27<sup>93</sup> being successful. In addition, throughout the year, the HR sector monitored and renewed contracts for contract and temporary agents and external providers.

The EDPS also participates in the EC's traineeship programme and recruits ten trainees twice a year. Due to the growing interest in this programme and the limited number of trainees assigned to the EDPS and the EDPB, the rotation system established in 2023 continued, allowing all services to benefit from it at regular intervals. The HRBA serves as a contact point for managing the programme internally, providing support to the recruiting units throughout the selection process, supervising quota allocation and distribution, coordinating logistics and organising information sessions for welcoming trainees.

In 2024, the HR team further improved the new on-boarding procedure introduced in 2023, based on the participant feedback, by adding a more interactive session that fostered engagement. Staff statistics are available in Annex 1 with reference date being 31 December 2024. As of 31 December 2024 the total number of active statutory staff was 146, compared to 141 on 31 December 2023.

## Budget

### Budget discharge

For the financial year 2022, the EDPS was granted discharge<sup>94</sup> by the European Parliament and the European Court of Auditors (ECA) did not identify any specific issues concerning the EDPS, as stated in its annual report<sup>95</sup>.

---

<sup>93</sup> For 9 officials, 15 contract and 3 a temporary agents.

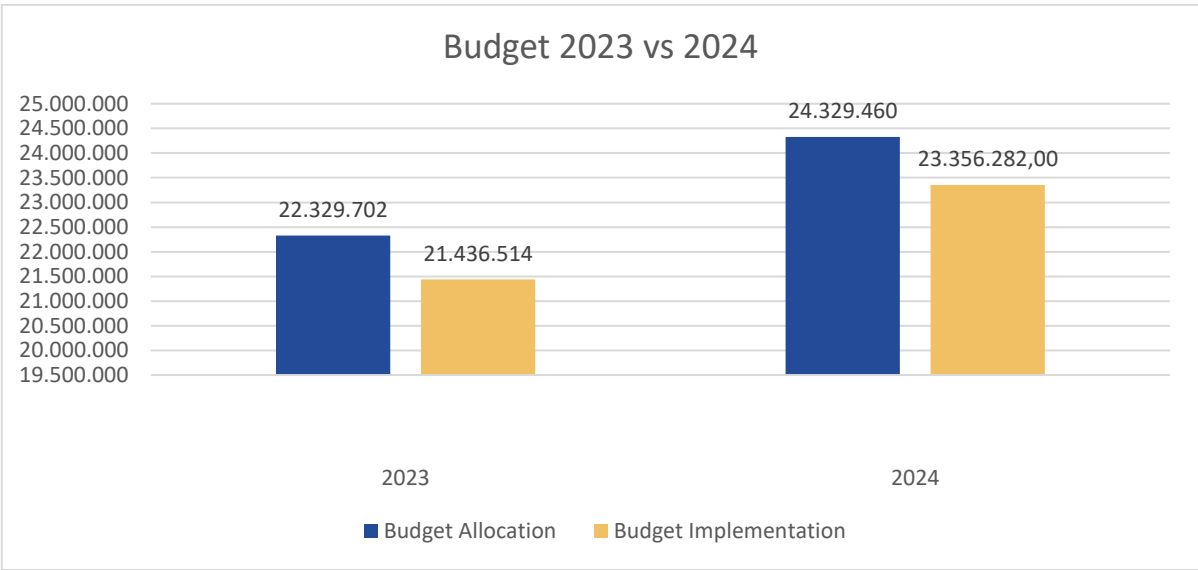
<sup>94</sup> European Parliament decision of 11 April 2024 on discharge in respect of the implementation of the general budget of the European Union for the financial year 2022, Section IX – European Data Protection Supervisor (2023/2138(DEC)) [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0235\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0235_EN.html)

<sup>95</sup> ECA annual report 2022 <https://www.eca.europa.eu/en/publications/AR-2022>

For the financial year 2023, the discharge procedure is ongoing, with results expected in May 2025. In its annual report<sup>96</sup> the ECA noted delays in receiving and verifying declarations concerning the rights for family and child allowances. For more details, please see section on [ECA](#).

## Budget allocation for 2024

The 2024 EDPS operating budget amounted to EUR 24 329 460, reflecting an increase of 7% compared to the final budget for 2023. This increase is largely attributed to anticipated higher expenditures under Title 1 (staff expenditure) and Title 2 (administrative expenditure).



## Budget implementation

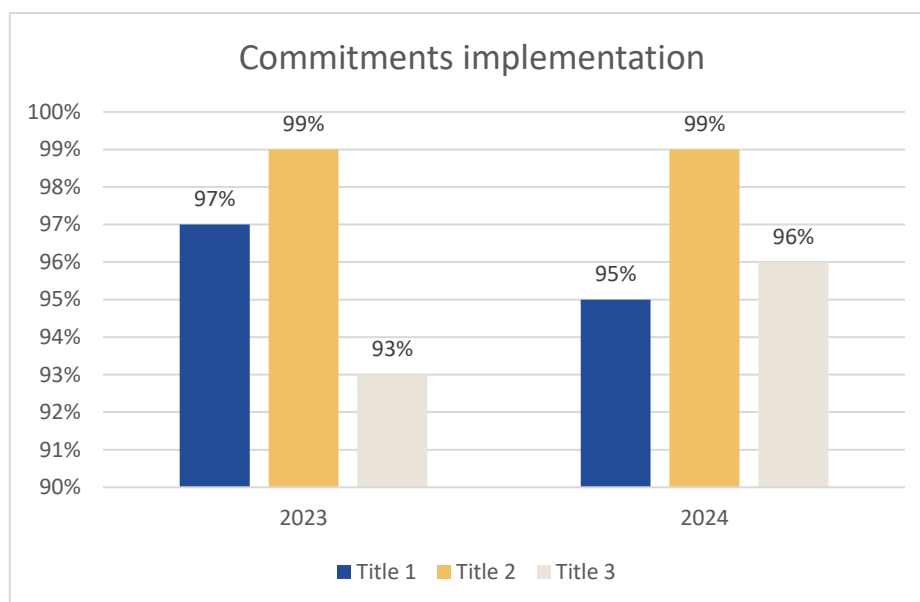
The overall budget achieved a 96% commitment appropriation implementation rate, reflecting rigorous monitoring and prudent financial management.

For Title 1, commitment appropriations were implemented at 95%. Savings resulted from a high number of local recruitments, reduced training activities and lower post-school services costs. However, staff-related expenses were affected by unexpected fluctuations and rising living costs.

Title 2 achieved an exceptional 99% implementation rate, reflecting effective resource allocation and expenditure monitoring. However, the expert reimbursement budget line had a lower implementation rate of 78%, primarily due to the increased use of hybrid meetings, which reduced travel and associated costs, while maintaining stakeholder engagement.

For Title 3, the implementation rate reached 96%. The shift to hybrid and virtual meeting formats for EDPB activities significantly reduced costs for travel, accommodation, venue rentals and catering compared to what was forecasted. Hybrid meetings also allowed broader participation from national Data Protection Authorities (DPAs) without incurring additional logistical costs, enhancing operational efficiency.

<sup>96</sup> ECA annual report 2023: <https://www.eca.europa.eu/en/publications/AR-2023>



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

## Draft budget for 2025

The 2025 budget exercise was successfully completed despite challenges from rising inflation and high living costs, ensuring the EDPS' priorities remain on track.

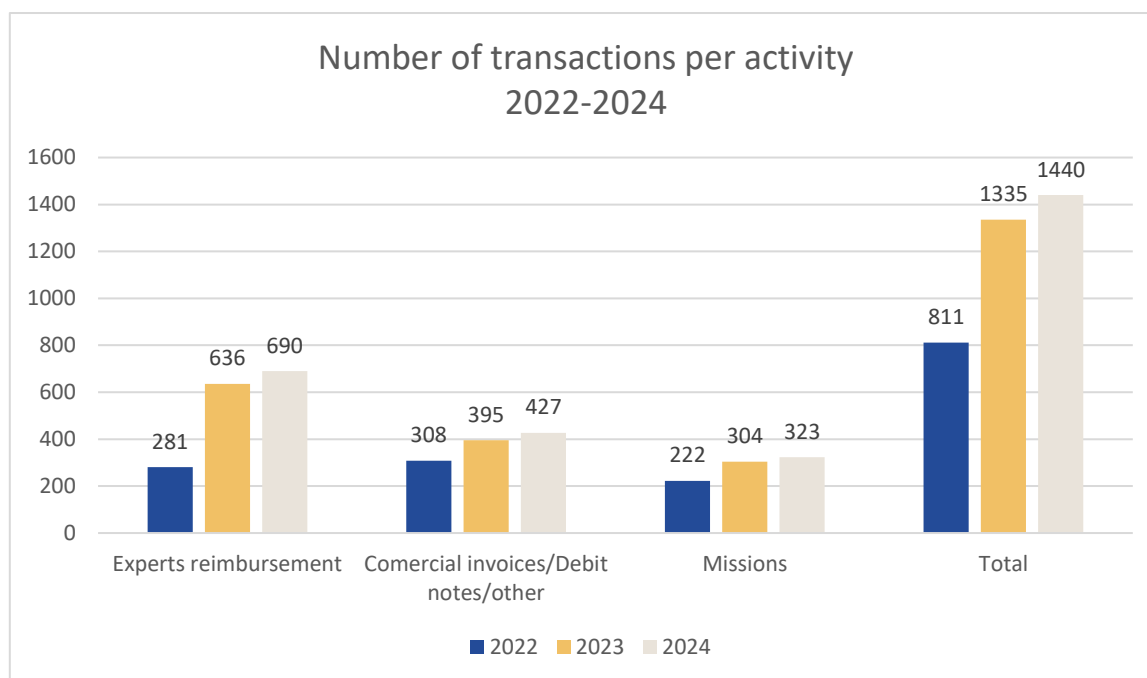
As in previous years, strict budgetary discipline for administrative expenditure and staffing across the EUIBAs was a key focus in drafting the 2025 budget. However, the EC and the Council imposed substantial cuts as part of broader savings measures for European administrations. This will require a reassessment of priorities, potentially leading to modifications or cancellations of planned initiatives.

Despite these constraints, the EDPS secured four additional posts for administrators and five posts for contract agents to support new responsibilities in Artificial Intelligence and Cybersecurity. The final approved budget reflects an 11.32% increase in expenditure compared to 2024.

## Finance

The number of payment transactions rose slightly in 2024, reaching 1 440, compared to 1 335 in 2023, representing a 7.87% increase. However, the number of transaction remained below 2019 levels, as certain activities were affected by the shift to new working methods, such as the organisation of virtual or hybrid experts' meetings or participation in virtual events.

In 2024, 96.87% of payments were processed on time, i.e. within 30 days.



Missions, expert payments and salaries are initiated by the Paymaster Office of the European Commission (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

In accordance with Art. 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 utilises checklists that outline the essential checks to be conducted by the operational and financial agents involved in processing operations. The use of the Speedwell<sup>97</sup> system significantly streamlines the aforementioned basic controls applied to payments and commitments.

## Procurement and contracting

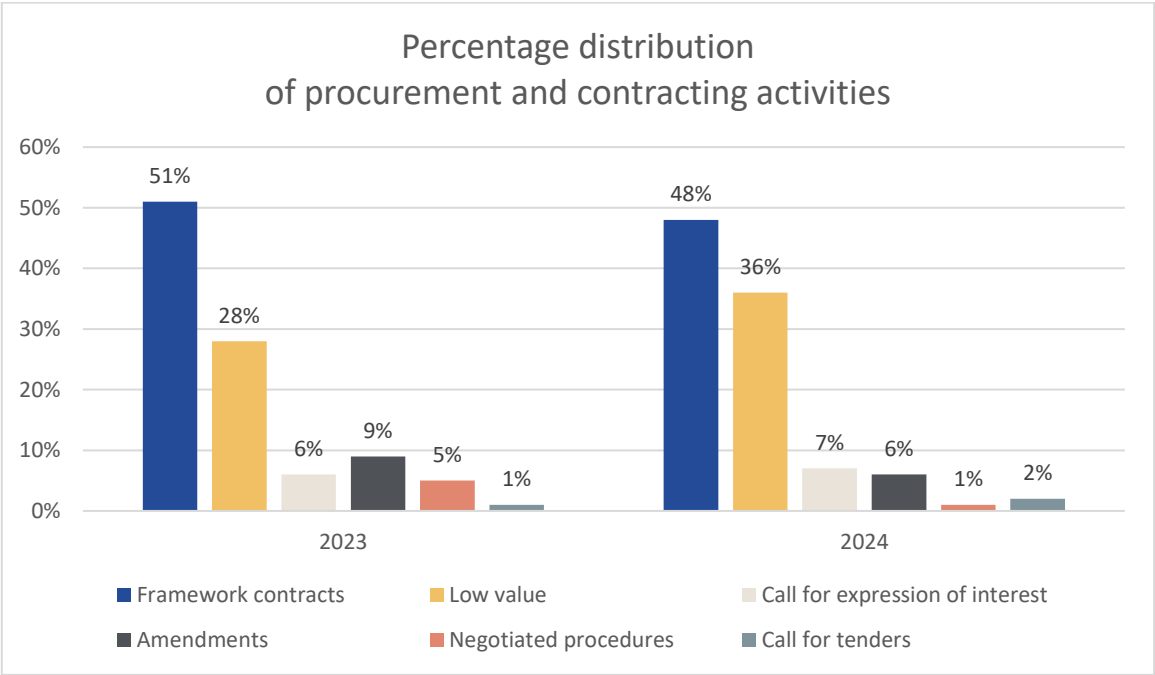
In 2024, the EDPS, acting as well on behalf of the EDPB, launched 126 public procurement procedures compared to 132 in 2023. This includes one direct service contract and two negotiated procedures without prior publication, which are reported in line with Art. 74,§10 of the Financial Regulation. Additionally, the

<sup>97</sup> Since 2020, the EDPS has been utilising 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 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.

EDPS managed a call for expression of interest to establish a list of individual experts for the EDPB, resulting in the award of nine specific contracts.

Similar to the previous year, the EDPS outsourced certain activities, such as events, conferences, and other projects, to external contractors. The HRBA supported both institutions in these procedures, which were mostly very low-value contracts (45). In 2024, the EDPS implemented a significant number of framework contracts (60), including inter-institutional agreements related to IT consultancy, communication activities, interim services and office supplies.

Throughout the public procurement procedure, the HRBA prioritised an open, fair, transparent selection and competition process, ensuring that external contractors meet high moral and ethical standards.



### Missions’ management

Missions’ management at the EDPS is conducted in accordance with the applicable rules of the European Commission. 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 HRBA unit oversees initiation, validation, and related information.

Missions 2021-2024				
	2021	2022	2023	2024



	Supervisor	Staff	Supervisor	Staff	Supervisor	Staff	Supervisor	Staff
<b>Nr. of missions</b>	6	57	21	171	24	246	23	218
<b>Average cost EUR</b>	446	505	1 488	1 035	1 303	998.61	1 681	852.76
<b>Total cost EUR</b>	2 675	28 789	31 267	176 903	31 279	284 580	38 672	18 5684

As regards the Supervisor, missions are conducted in full transparency as provided in the Code of conduct.

Number of missions and cost in 2024	
EDPS Supervisor Wojciech Rafał Wiewiórowski	
<b>Number of missions</b>	23
<b>Cost (EUR)</b>	38 672

Full details on the Supervisor's missions for 2024 can be found in [Annex 3](#).

In May 2024, EDPB elected a new Chair, Ms Anu Talus who performed 17 missions since, and her deputy two.

Number of missions and cost in 2024		
EDPB Chair		
Chair name	Number of missions	Cost (EUR)
<b>Anu Talus</b>	17	42 563
<b>Irini Loizidou-Nikolaidou (deputy)</b>	2	2 359

## IT infrastructure and tools

The EDPS Digital Transformation sector (hereinafter 'the Sector') oversees IT services and infrastructure through Memoranda of Understanding (MoUs) and Service Level Agreements (SLAs) with the EC and EP, manages critical applications like the Website Evidence Collector (WEC) and leads digital transformation projects.

The MoU with the EP covers essential IT infrastructure<sup>98</sup>, while the one with the EC includes hosting in the DIGIT data centre, access to specific services<sup>99</sup>. The Sector is the single point of contact with service providers, ensuring good communication keep interoperability among all services. Furthermore, the Sector acts as internal solution provider for designing and operating business-specific applications that cannot be covered through MoUs/SLAs.

The EDPS Public Key Infrastructure (PKI) supports secure access to the Case Management System (CMS). A successful PKI redeployment test took place in 2023. However, sourcing and operational delays postponed the new PKI's rollout to 2025.

Following a pilot of the Nextcloud collaborative platform<sup>100</sup> with a European cloud service provider, the EDPS decided to migrate it to an EC-managed internal data centre. In parallel, the openDesk platform was explored, but to accelerate migration, the , an EDPS prioritised Nextcloud. By end-2024, migration was nearly complete, with minor hosting issues remaining.

In 2024, the EDPS released the Website Evidence Collector (WEC) version 2.1.2 and a major upgrade, version 3.0, focused on usability for non- technical users. These tools help data controllers, processors and authorities in identifying website tracking operations. Additionally, the EDPS launched WEC Online, a centrally hosted, open-source tool for DPOs and controllers. It became operational in late 2024, with a production version expected in early 2025.

To raise awareness of AI risks, the EDPS developed a deepfake demonstration tool for conferences in 2023. Maintenance in 2024 ensured compatibility with new AI models.

The EDPS completed pilots of Mastodon and PeerTube-based platforms, supporting institutional migrations. Meanwhile, the EDPS began transitioning EDPS-owned accounts to a production-grade instance but, procurement delays and cloud provider issues postponed completion to 2025.

The CMS, operational since 2013, was co-developed with EP and tailored to EDPS needs with robust data protection safeguards. Ongoing support is provided under the SIDE Framework Contracts since 2015. Annual assessments are conducted based on provider documentation and audits.

In 2024, the EDPS deployed **EU Send** for secure transmission of sensitive, non-classified information across EUIBAs, particularly for breach notifications and supervision. Feasibility and security testing occurred in late 2023. Originally developed by the EC (formerly eTrust-EX), the platform has been accessible to the EDPS since 2016, for receiving documents.

To enhance service delivery the EDPS adopted the EP's Service Now, an IT support ticketing system, introducing automated workflows aim to reduce email exchanges and introduce measurable KPIs. The EDPS also explored streamlining internal processes with automated workflows and custom web portal forms using EC systems. A proof of concept was developed for data breach notifications.

Finally, in 2024, the EDPS collaborated with the EP to anticipate the end of support for Microsoft Office 2016 and Windows 10. However, due to delays in the EP's migration strategy, the EDPS could not finalise its own by the end of 2024 either.

---

<sup>98</sup> Network services, communications, computers, intranet, shared drives, Outlook, video conferencing, and office suites

<sup>99</sup> ARES, ABAC Assets, AGM, EU Login, EU Send, EC Framework Contracts, and the web portal

<sup>100</sup> 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.

## Cybersecurity, Information Security, Physical Security and Business Continuity

In January 2024 the Cybersecurity Regulation 2023/2841<sup>101</sup> came into effect. As a result, the EDPS has undertaken a range of compliance activities, including the appointment of the Local Cybersecurity Officer (LCO) and the planning and implementation of specific measures in accordance with guidelines issued by the Inter-Institutional Cybersecurity Board (IICB) and CERT-EU. These measures take into account the EDPS's status as a small institution with significant dependencies on services provided by the European Parliament and the Commission. Consequently, the compliance activities focus on assets and domains directly managed by the EDPS such as personnel, access control, security incidents and Service Level Agreements with external service providers.

Moreover, the management of information security, physical security, business continuity, and security of classified information remains crucial in protecting the EDPS's mission, reputation and business continuity from associated risks. To support this, the independent roles of the Local Information Security Officer (LISO), and the Local Security Officer (LSO) have been established. Both the LISO and the LSO report directly to the EDPS Secretary General, ensuring their independence and autonomy.

During 2024, a number of activities were performed in the areas of cybersecurity, information security, physical security and business continuity:

- Management of Restricted lapTOPs (RTOP), for EDPS staff processing EU classified information (EUCI).
- Organisation and conduct of Business Continuity exercises such as building evacuation and business continuity plan quiz.
- Management of the EP-CRISIS and EU-WARN for the staff of EDPS and EDPB.
- Security and cybersecurity trainings for all EDPS staff and phishing exercise for all EDPS and EDPB staff.
- Management and resolution of incidents impacting information security, physical security, business continuity and cybersecurity.

## Internal control

### Control results

#### Effectiveness

##### 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 ECA. To reach this conclusion, the EDPS reviewed the results of the key controls

---

<sup>101</sup> Regulation (EU, Euratom) 2023/2841: <https://eur-lex.europa.eu/eli/reg/2023/2841/oj/eng>

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 authorising officer by delegation (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 486 589 (2% of the 2024 budget after transfers)

## Ethics

The EDPS prioritises professional ethics, promoting excellence in the European civil service and safeguarding the framework of rights and obligations outlined in the Staff Regulations. To guide staff conduct, the EDPS has established an ethics framework, comprising a Code of conduct for the Supervisor 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 Code of conduct, the Supervisor publishes an annual declaration of interest<sup>102</sup>.

New staff members attend a mandatory presentation on the ethics framework and on anti-harassment policy during on boarding. In 2024, two on boarding sessions were held for 26 newcomers.

During 2024, the EDPS Ethics officer, staff member in charge of coordinating activities related to ethics, advised staff on ethical matters and received 28 formal requests (against 26 in 2023) related to the Code of Conduct for staff. The majority of requests concerned the authorisation for carrying out external activities (in particular lectures, presentations and patronage) and publications. To enhance the robustness of related administrative processes, an e-workflow for ethics requests from the EDPB staff was integrated into Sysper, mirroring the Commission's ethics module. One case of ethical misconduct was transmitted to the Investigation and Disciplinary Office of the European Commission (IDOC), which opened an administrative inquiry on behalf of the EDPS. The conclusion of the inquiry is expected beginning of 2025.

---

<sup>102</sup> Declaration of interests of the Supervisor, [29 January 2024](#) and update of [19 September 2024](#)

One European Ombudsman (EO) inquiry was closed during the reference year with no further findings, while another, ongoing since 2023, was closed with a maladministration finding<sup>103</sup>.

The maladministration finding referred to EDPS' failure to complete its assessment of a complaint within a reasonable timeframe and for not having proactively informed the complainant about the case's progress. In response to the EO's decision, the EDPS issued a formal apology and improved its procedures. Staff are now required to proactively update complainants, including explaining delays. Additionally, the EDPS will clarify its obligation to suspend investigations under Article 16(6) of its Rules of Procedure when awaiting court rulings or decisions from other bodies on the same matter.

Notably, the EDPS was not involved in any investigations carried out by the European Anti-fraud Office (OLAF) in 2024, indicating a positive ethical climate within the organisation. Overall, the EDPS remains committed to upholding the highest standards of professional ethics and integrity.

### Deviations' reporting

All deviations are signed by the authoring officer in charge. In 2024, 14 events were recorded: ten derogations<sup>104</sup>, two exceptions and two non-compliance events<sup>105</sup>. Compared to 2023 (12 events), the overall number of deviations increased.

### Accounting controls

The European Commission's (EC) 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 Service Level Agreements (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.

### Ex-post

According to Art. 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. Following an ECA observation (see section on [ECA](#)) and due to the fact that the organisation grew over the years with an increasing budget and number of financial transactions, the EDPS Secretary-General, decided to carry out again these controls, as from 2022. In Q1 2025, the EDPS updated the ex-post control procedure integrating the risk assessment approach and clarifying the sampling methodology.

For 2024, the ex-post controls were carried out following a risk assessment which resulted in selecting the HR process for establishing the grade for staff members. Five files were selected of various grades and functions and types of contract, representing 1/6 of all files.

One error resulted in an incorrect grade assignment, leading to a quantifiable error of EUR 1 788.36, which, without extrapolation to the whole population, remains below the [materiality threshold](#). In addition, the

---

<sup>103</sup> 1. 801/2024/TM (closed), 2. CASE 1888/2023/TM (closed with maladministration finding).

<sup>104</sup> Derogations are explicit situations allowed or foreseen in the processes and procedures under specific circumstances.

<sup>105</sup> Exceptions are deviations which are not initially foreseen by the procedures and therefore require individual follow-up. They may take a form of the management's overriding of prescribed processes or procedures, allowing for actions that go against the results of previous controls. If such control-overrides or deviations are approved before action is taken (ex-ante), they are called 'exceptions'.

erroneous amount will be corrected retroactively; therefore, there is no impact on the EDPS budget. The EDPS action plan will focus on staff training, establishment of procedures and further enhancing the automated tool used.

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 2024, 96.87% of payments were processed on time (within 30 days). In addition, 96% of the budget was executed against a target of 90%, as set in the KPI nr. 9. For carrying out a cost-benefit analysis, the EDPS, being a small Institution, takes as a base the model applied by EPSO, since this office, as the EDPS, 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 2024 would be EUR 820 354. The total budget implementation in terms of payments for 2024 is EUR 20 712 599. This means that the cost of the control activities represents 3.96% of the EDPS expenditure.

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 2024, the Internal Audit Service (IAS) initiated one audit, and the European Court of Auditors (ECA) completed its Statement of Assurance (SoA) for the 2023 financial year. At the end of Q1 2025, the EDPS submitted to the IAS one recommendation for review. The 2023 SoA gave rise to one non-quantifiable finding, while the 2024 SoA is ongoing. Details follow in dedicated sections below.

### Internal Audit Service

In April 2024, the IAS launched the audit on ‘governance arrangements for information technology (IT) services provided by the European Parliament (EP) to the EDPS’. The results of this audit, at the end of Q1 2025, are underway.

In 2023, the IAS carried out the audit on the ‘methodology for the planning of the EDPS audits in the EDPS’ and issued the following two recommendations:

Recommendation	Risk rate	Implementation deadline
1. Design of the methodology to establish the EDPS audit plan	Very important	30/04/2025
2. Implementation of the EDPS audit plan	Important	31/12/2024

Concerning the very important finding, the IAS concluded that the methodology used to establish the audit plan was not clear and/or up to date as regards certain aspects such as roles and responsibilities of the actors involved. The planning process did not involve the clear identification of the “audit universe”, which constitutes the starting point for a structured risk assessment. Furthermore, the methodology did not encompass a risk-based method for prioritising audits (including setting up an audit frequency, when relevant)

based on an objective assessment of the likelihood and severity of risks. Finally, there was not an adequate process in place for estimating the human resources needed to implement the audit plan and neither a long-term audit strategy.

According to its action plan, the EDPS mitigating actions involve the update of the case manual on audits for clarifying roles and responsibilities and the strengthening of the risk-based approach through the regular review of comprehensive lists of EUIBAs registers of processing activities and the use of business intelligence tools and surveys. In addition, the assessment of the likelihood and severity of risks will be defined using the EDPS DPIA list combined with other sources of information, eg. volume of processing activities etc. Depending on the priorities to be set by the new Supervisor the EDPS will complement the audit long-term strategic perspective. The EDPS action plan was approved by the IAS in December 2023.

Regarding the implementation of the EDPS audit plan (recommendation nr. 2), EDPS completed it and submitted it to the IAS for review.

## European Court of Auditors

In October 2024, the European Court of Auditors (ECA) published its 2023 Annual Report<sup>106</sup>, in which the EDPS is featured in Chapter 10, "European public administration". The ECA had sampled one transaction on salaries, which revealed a non-quantifiable error. Specifically, the auditors found delays in receiving and verifying declarations concerning family and child allowances, that increases the risk of undue payments (Art.67 of Staff Regulation). Although the Staff Regulations place the responsibility on staff members to inform the institution of any changes that may affect allowances, the EDPS took proactive measures to mitigate this risk. Concretely, the EDPS promptly introduced a periodic reminder to staff, in the form of a communication, to declare any changes that may be applicable.

Regarding the follow-up on previous observations, the ECA closed the pending observation on ex-post controls, but will continue to closely monitor this process to ensure its effectiveness—including the updated ex-post controls procedure—during future audits. For more information on the ex-post controls see [here](#).

The 'Statement of Assurance' audit for year 2024 was initiated in Q4 2024 and is scheduled to be finalised in July 2025. For the moment, the ECA audited one salary payment and its examination did not give rise to any observations.

## Annual planning and risk management

The objectives are defined in the Strategy and reflected in the Annual Management Plan (AMP) in the form of concrete actions and deliverables throughout the coming year. The MP plan translates the EDPS long-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 MP. The procedure on the 'Strategic planning and programming cycle', mapping and giving concrete structure to the process is expected to be finalised in 2025.

The MP also includes key performance indicators (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 2024.

---

<sup>106</sup> 2023 Annual Report of the European Court of Auditors, 10 October 2024: [https://www.eca.europa.eu/ECAPublications/AR-2023/AR-2023\\_EN.pdf](https://www.eca.europa.eu/ECAPublications/AR-2023/AR-2023_EN.pdf)



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. Results of the 2025 exercise are expected in Q2 2025.

## 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 2024 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 7, ICS 8, and ICS 14.

In response to the latest Staff Satisfaction Survey (SSS), a working group was formed to analyse results and propose improvement actions. These were incorporated into an action plan, leading to enhancements in training and development (ICS 4 – Staff Evaluation and Development). Additionally, improvements in knowledge management contributed to better document management (ICS 11).

## 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's 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's 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's 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.

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 gives 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 here which could harm the interests of the institution.

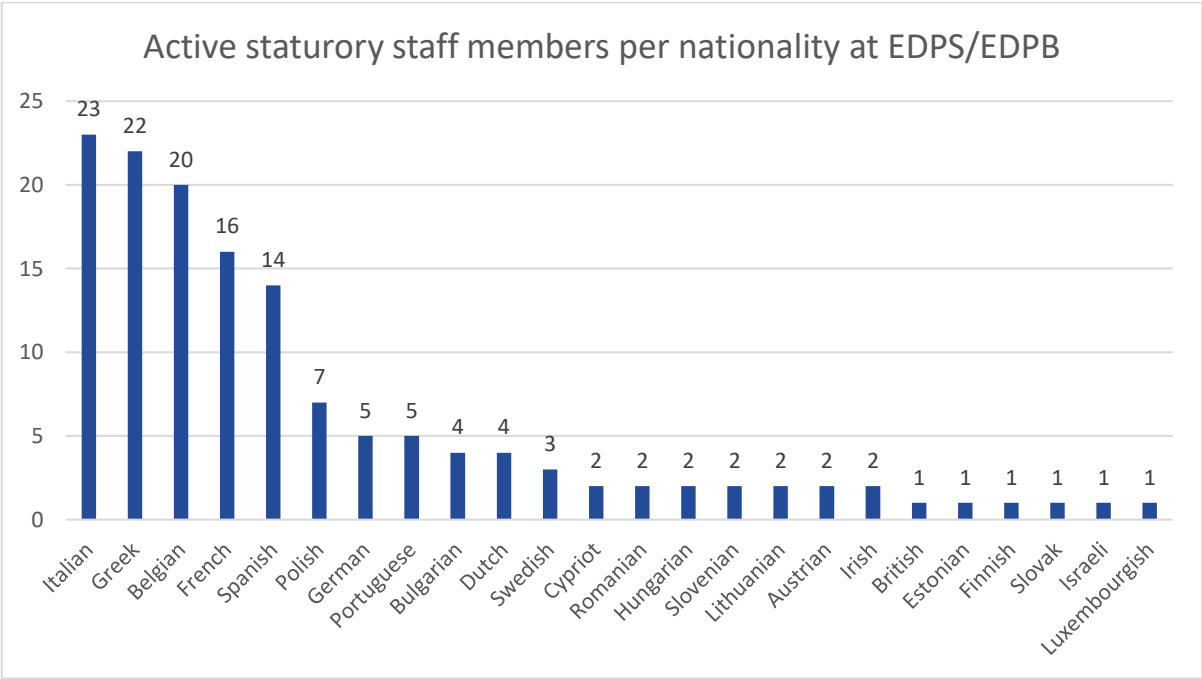
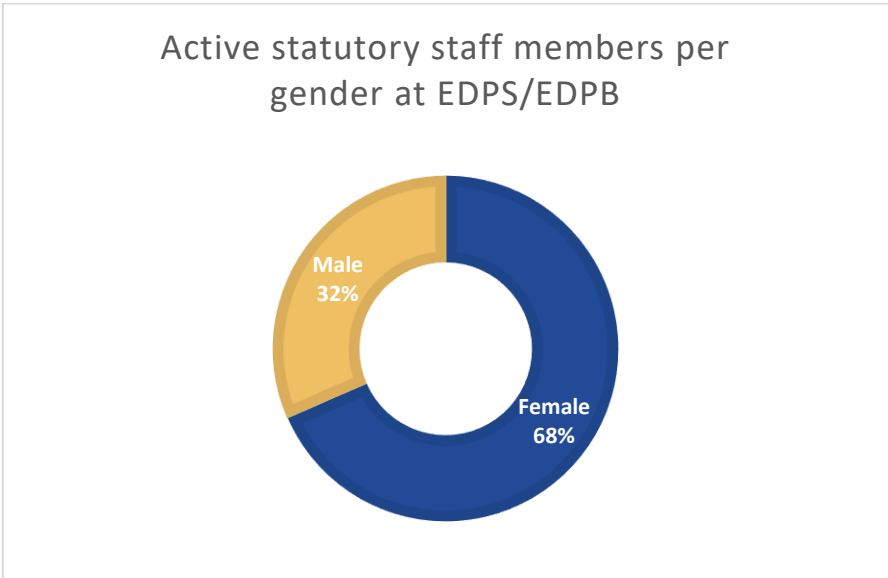
*e-signed*

in Brussels

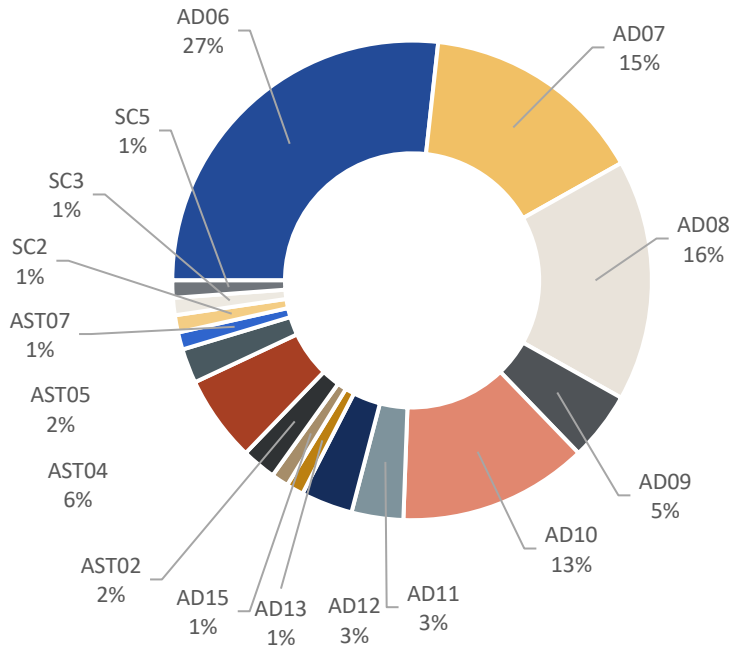
# Annexes

## Human resources at the EDPS/EDPB

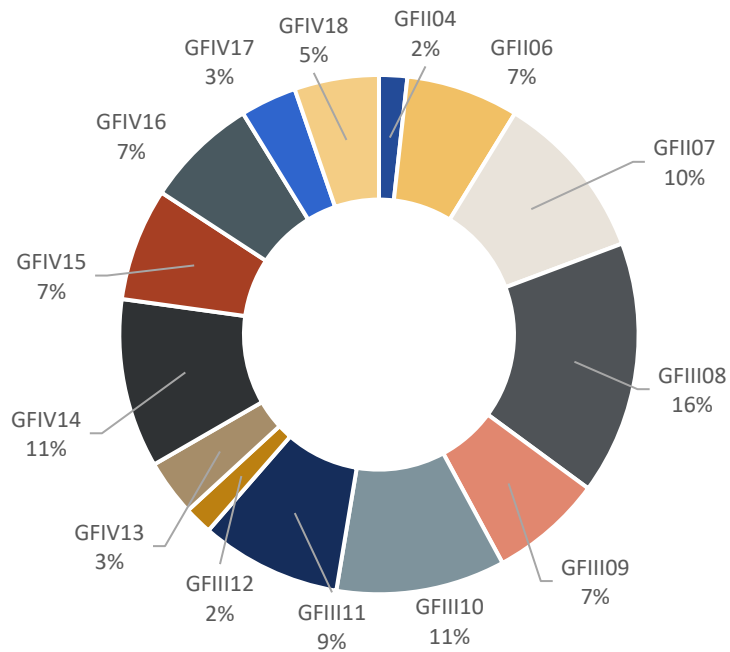
The charts below provide a snapshot of the situation on 31 December 2024.



## Officials and Temporary Agents



## Contract Agents per grade



**Budget in 2024**

TITLE 1 - EXPENDITURE RELATING TO PERSONS WORKING WITH THE INSTITUTION		2023 (after transfers)	execution 2023 (%)	2024 (after transfers)	2024 vs 2023	2024 vs 2023 (%)	execution 2024 (%)
<b>Chapter 10</b>	<b>Members of the institution</b>						
<b>Article 100</b>	<b>Remuneration, allowances and other entitlements of Members</b>						
	Item 1000 Remuneration and allowances	404.065,66	100,00%	436.000,00	31.934,34	7,90%	97,61%
	Item 1001 Entitlements on entering and leaving the service	0,00		2.650,00	2.650,00		99,89%
	Item 1002 Temporary allowances	0,00		0,00	0,00		
	Item 1003 Pensions	0,00		0,00	0,00		
	Item 1004 Provisional appropriation	0,00		0,00	0,00		
	<b>TOTAL Article 100</b>	<b>404.065,66</b>	<b>100,00%</b>	<b>438.650,00</b>	<b>34.584,34</b>	<b>8,56%</b>	<b>97,62%</b>
<b>Article 101</b>	<b>Other expenditure in connection with Members</b>						
	Item 1010 Further training	2.012,75	100,00%	0,00	-2.012,75	-100,00%	0,00%
	Item 1011 Mission expenses, travel expenses and other ancillary expenditure	33.921,59	100,00%	43.000,00	43.000,00	126,76%	100,00%
	<b>TOTAL Article 101</b>	<b>35.934,34</b>	<b>100,00%</b>	<b>43.000,00</b>	<b>7.065,66</b>	<b>19,66%</b>	<b>97,84%</b>
	<b>TOTAL Chapter 10</b>	<b>440.000,00</b>	<b>100,00%</b>	<b>481.650,00</b>	<b>41.650,00</b>	<b>9,47%</b>	<b>97,84%</b>
<b>Chapter 11</b>	<b>Staff of the institution</b>						
<b>Article 110</b>	<b>Remuneration, allowances and other entitlements of officials and temporary staff</b>						
	Item 1100 Remuneration and allowances	7.724.420,00	99,36%	8.713.350,00	988.930,00	12,80%	95,74%
	Item 1101 Entitlements on entering, leaving the service and on transfer	80.000,00	0,71%	85.000,00	5.000,00	6,25%	50,55%
	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		
	<b>TOTAL Article 110</b>	<b>7.804.420,00</b>	<b>98,35%</b>	<b>8.798.350,00</b>	<b>993.930,00</b>	<b>12,74%</b>	<b>95,30%</b>
<b>Article 111</b>	<b>Other staff</b>						
	Item 1110 Contract staff	2.020.500,00	96,32%	2.247.594,00	227.094,00	11,24%	97,51%
	Item 1111 Cost of traineeships and staff exchanges	325.000,00	59,96%	245.000,00	-80.000,00	-24,62%	84,06%
	Item 1112 Services and work to be contracted out	57.000,00	66,67%	60.000,00	3.000,00	5,26%	90,92%
	<b>TOTAL Article 111</b>	<b>2.402.500,00</b>	<b>90,70%</b>	<b>2.552.594,00</b>	<b>150.094,00</b>	<b>6,25%</b>	<b>96,07%</b>
<b>Article 112</b>	<b>Other expenditure in connection with staff</b>						
	Item 1120 Mission expenses, travel expenses and other ancillary expenditure	195.000,00	100,00%	150.000,00	-45.000,00	-23,08%	100,00%
	Item 1121 Recruitment costs	5.000,00	100,00%	10.000,00	5.000,00	100,00%	50,00%
	Item 1122 Further training	40.091,11	73,30%	89.000,00	48.908,89	121,99%	60,59%
	Item 1123 Social service	0,00	0,00%	0,00	0,00		0,00%
	Item 1124 Medical service	13.000,00	100,00%	30.000,00	17.000,00	130,77%	64,48%
	Item 1125 Union nursery centre and other day nurseries and after-school centres	66.581,00	100,00%	100.000,00	33.419,00	50,19%	79,28%
	Item 1126 Relations between staff and other welfare expenditure	72.327,89	100,00%	21.000,00	-51.327,89	-70,97%	57,00%
	<b>TOTAL Article 112</b>	<b>392.000,00</b>	<b>97,27%</b>	<b>400.000,00</b>	<b>8.000,00</b>	<b>2,04%</b>	<b>79,88%</b>
	<b>TOTAL Chapter 11</b>	<b>10.598.920,00</b>	<b>96,57%</b>	<b>11.750.944,00</b>	<b>1.152.024,00</b>	<b>10,87%</b>	<b>94,94%</b>
	<b>TOTAL TITLE 1</b>	<b>11.038.920,00</b>	<b>96,71%</b>	<b>12.232.594,00</b>	<b>1.193.674,00</b>	<b>10,81%</b>	<b>95,06%</b>

TITLE 2 - BUILDINGS, EQUIPMENT AND EXPENDITURE IN CONNECTION WITH THE OPERATION OF THE INSTITUTION		2023 (after transfers)	execution 2023 (%)	2024 (after transfers)	2023 vs 2022	2023 vs 2022 (%)	execution 2023 (%)
Chapter 20	Buildings, equipment and expenditure in connection with the operation of the institution						
Article 200	Rents, charges and buildings expenditure	1.731.857,00	100,00%	1.751.494,00	19.637,00	1,13%	100,00%
	<b>TOTAL Article 200</b>	<b>1.731.857,00</b>	<b>100,00%</b>	<b>1.751.494,00</b>	<b>19.637,00</b>	<b>1,13%</b>	<b>100,00%</b>
Article 201	Expenditure in connection with the operation and activities of the institution						
	Item 2010 Information technology equipment and services	820.000,00	99,21%	911.620,00	91.620,00	11,17%	99,21%
	Item 2011 Furnitures, office supplies and telecommunication costs	12.000,00	100,00%	12.000,00	0,00	0,00%	100,00%
	Item 2012 Other operating expenditure	235.000,00	98,40%	458.884,00	223.884,00	95,27%	98,40%
	Item 2013 Translation and interpretation costs	551.000,00	100,00%	190.000,00	-361.000,00	-65,52%	100,00%
	Item 2014 Expenditure on publishing and information	186.000,00	98,42%	140.888,14	-45.111,86	-24,25%	98,42%
	Item 2015 Expenditure in connection with the activities of the institution	146.000,00	96,81%	225.227,86	79.227,86	54,27%	96,81%
	Item 2016 Experts reimbursements	25.000,00	78,88%	45.000,00	20.000,00	80,00%	78,88%
	<b>TOTAL Article 201</b>	<b>1.975.000,00</b>	<b>98,73%</b>	<b>1.983.620,00</b>	<b>8.620,00</b>	<b>0,44%</b>	<b>98,12%</b>
	<b>TOTAL CHAPTER 20</b>	<b>3.706.857,00</b>	<b>99,38%</b>	<b>3.735.114,00</b>	<b>28.257,00</b>	<b>0,76%</b>	<b>99,00%</b>
	<b>TOTAL TITLE 2</b>	<b>3.706.857,00</b>	<b>99,38%</b>	<b>3.735.114,00</b>	<b>28.257,00</b>	<b>0,76%</b>	<b>99,00%</b>



TITLE 3 - EUROPEAN DATA PROTECTION BOARD (EDPB)		2023 (after transfers)	execution 2023 (%)	2024 (after transfers)	2023 vs 2022	2023 vs 2022 (%)	execution 2023 (%)
<b>Article 300 Rents, charges and buildings expenditure</b>							
Item 3000 Rents, charges and buildings expenditure		692.768,85	100,00%	704.223,40	11.454,55	1,65%	100,00%
<b>TOTAL Article 300</b>		<b>692.768,85</b>	<b>100,00%</b>	<b>704.223,40</b>	<b>11.454,55</b>	<b>1,65%</b>	<b>100,00%</b>
<b>Article 301 Remuneration, allowances and other entitlements of officials and temporary staff</b>							
Item 3010 Remuneration and allowances		2.236.013,15	82,50%	2.411.500,00	175.486,85	7,85%	94,56%
Item 3011 Entitlements on entering, leaving the service and on transfer		26.000,00	28,94%	30.000,00	4.000,00	15,38%	82,80%
Item 3012 Allowances and miscellaneous contributions in connection with early termination of service							
<b>TOTAL Article 301</b>		<b>2.262.013,15</b>	<b>81,89%</b>	<b>2.441.500,00</b>	<b>179.486,85</b>	<b>7,93%</b>	<b>94,41,00%</b>
<b>Article 302 Other staff</b>							
Item 3020 Contract staff		1.553.000,00	99,71%	1.734.152,00	181.152,00	11,66%	98,40%
Item 3021 Cost of traineeships and staff exchanges		35.000,00	92,70%	37.000,00	2.000,00	5,71%	100,00%
Item 3022 Services and work to be contracted out		100.000,00	81,79%	60.000,00	-40.000,00	0,00%	99,02%
<b>TOTAL Article 302</b>		<b>1.688.000,00</b>	<b>98,50%</b>	<b>1.831.152,00</b>	<b>143.152,00</b>	<b>8,48%</b>	<b>98,45%</b>
<b>Article 303 Other expenditure in connection with staff of the Board</b>							
Item 3030 Mission expenses, travel expenses and other ancillary expenditure		49.500,00	100,00%	57.500,00	8.000,00	16,16%	100,00%
Item 3031 Recruitment costs		3.000,00	66,67%	3.000,00	0,00	0,00%	100,00%
Item 3032 Further training		24.000,00	77,09%	36.000,00	12.000,00	50,00%	67,48%
Item 3033 Medical service		5.000,00	100,00%	15.000,00	10.000,00	200,00%	59,08%
Item 3034 Union nursery centre and other day nurseries and after-school centres		18.500,00	100,00%	35.000,00	16.500,00	89,19%	93,00%
<b>TOTAL Article 303</b>		<b>100.000,00</b>	<b>93,50%</b>	<b>146.500,00</b>	<b>46.500,00</b>	<b>46,50%</b>	<b>86,15%</b>
<b>Article 304 Expenditure in connection with the operation and activities of the Board</b>							
Item 3040 EDPB plenaries and sub-group meetings		332.000,00	78,53%	307.051,60	-24.948,40	-7,51%	92,93%
Item 3041 Translation and interpretation costs		839.000,00	99,27%	800.108,00	-38.892,00	-4,64%	93,91%
Item 3042 Expenditure on publishing and information		110.000,00	89,60%	126.400,00	16.400,00	14,91%	90,09%
Item 3043 Information technology equipment and services		935.000,00	99,62%	1.281.617,00	346.617,00	37,07%	99,41%
Item 3044 Furnitures, office supplies and telecommunication costs		7.000,00	44,04%	12.000,00	5.000,00	71,43%	15,14%
Item 3045 External consultancy and studies		660.000,00	97,63%	312.000,00	-348.000,00	-52,73%	99,86%
Item 3046 Other expenditure in connection with the activities of the EDPB		180.000,00	91,11%	196.700,00	16.700,00	9,28%	80,10%
Item 3047 Other operating expenditure		110.000,00	100,00%	152.500,00	42.500,00	38,64%	99,71%
Item 3048 EDPB Chair and Vice chairs expenses		50.000,00	95,10%	50.000,00	0,00	0,00%	100,00%
<b>TOTAL Article 304</b>		<b>3.223.000,00</b>	<b>95,95%</b>	<b>3.238.376,60</b>	<b>15.376,60</b>	<b>0,48%</b>	<b>95,65%</b>
<b>TOTAL CHAPTER 30</b>		<b>7.965.782,00</b>	<b>92,82%</b>	<b>8.361.752,00</b>	<b>395.970,00</b>	<b>4,97%</b>	<b>96,10%</b>
<b>TOTAL TITLE 3</b>		<b>7.965.782,00</b>	<b>92,82%</b>	<b>8.361.752,00</b>	<b>395.970,00</b>	<b>4,97%</b>	<b>96,10%</b>
<b>TOTAL BUDGET</b>		<b>22.711.559,00</b>	<b>95,78%</b>	<b>24.329.460,00</b>	<b>1.617.901,00</b>	<b>7,12%</b>	<b>96,02%</b>

## List of missions undertaken by the Supervisor in 2024

Missions undertaken by the Supervisor in 2024				
Wojciech Rafał Wiewiórowski				
	Date from	Date to	Purpose	Cost (EUR)
1.	26/11/2024	842.91	DPO Network Luxembourg, - Seminar at Utrecht University, LUX, NDL	842.91
2.	12/11/2024	2 030.57	Data Protection Workshop, Paris, 13 November 2024 - Florence Keynote speaker during our forthcoming conference on "The EU's Area of Freedom Security and Justice in the Digital Age - 14 - 15 November 2024, FRA, ITA	2 030.57
3.	28/10/2024	3 869.47	46th Global Privacy Assembly Jersey Channel Islands, GBR	3 869.47
4.	09/10/2024	1 350.76	G7 Privacy Italia 2024 "PRIVACY IN THE ERA OF DATA", ITA	1 350.76
5.	21/09/2024	5 422.57	International Organisations Workshop on Data Protection at World Bank in Washington, USA	5 422.57
6.	16/09/2024	530.67	EDEN Conference 2024 - Data Protection & Cyber Security as Law Enforcement Core Business, NDL	530.67
7.	12/09/2024	1 110.44	Forum for EU-US Legal-Economic Affairs, Paris, FRA	1 110.44
8.	02/09/2024	1 067.30	IPEN meeting Karlstad and ENISA event, DEU	1 067.30
9.	26/08/2024	61.56	Invitation to Campus Poland of the Future 2024, POL	61.56
10.	01/07/2024	876.40	PL&B's 37th Annual International conference at St. John's College, GRB	876.40

11.	23/06/2024	648.23	International Conference Personal Data Protection: building the future, Lisbon, PRT	648.23
12.	03/06/2024	1 080.44	Conference Personal data protection in the European Union, POL	1 080.44
13.	28/05/2024	1 867.72	Forum for EU-US Legal-Economic Affairs, USA	1 867.72
14.	13/05/2024	997.22	Spring Conference 2024, LTU	997.22
15.	22/04/2024	4 674.27	Aniversario del INFOEM Mexico, MEX	4 674.27
16.	01/04/2024	6 048.02	IAPP Global Privacy Summit and DPA Day, USA	6 048.02
17.	27/03/2024	166.45	Speaker invitation - inCyber Forum (FIC) , Lille, FRA	166.45
18.	18/03/2024	945.95	Conference on Artificial Intelligence and Its Legal Implications, POL	945.95
19.	10/03/2024	1 011.11	Invitation to the Fundamental Rights Forum, AUT	1 011.11
20.	29/02/2024	145.28	Lecture at Leiden University, DEU	145.28
21.	19/02/2024	159.12	PARLEU2024BE - JPSG meeting, BEL	159.12
22.	07/02/2024	3 539.02	Visit to Cambridge, MA (USA)	3 539.02
23.	11/01/2024	226.56	Jean Monnet House training for EDPS managers, FRA	226.56
<b>Total:</b>				<b>38 672.04</b>