EDPS

EUROPEAN
DATA PROTECTION
SUPERVISOR



ANNUAL REPORT

2024



An executive summary of the Annual Report 2024, which gives an overview of the key developments of EDPS activities in 2024, is also available.

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

The website also details a subscription feature to our newsletter.

Brussels, Belgium: PWC EU Services EEIG

© Design and Photos: PWC EU Services EEIG, EDPS & European Union

© European Union, 2024

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the European Data Protection Supervisor copyright, permission must be sought directly from the copyright holders.

PRINT ISBN 978-92-9242-898-3 ISSN 1830-5474 doi: 10.2804/4430975 QT-01-25-000-EN-C

PDF ISBN 978-92-9242-897-6 ISSN 1830-9585 doi: 10.2804/9599117 QT-01-25-000-EN-N

Table of Contents

Foreword	**1**
Presenting the EDPS	**3**
Highlights of 2024	**7**
Supervision & Enforcement: consistent data protection in EU institutions	**12**
Policy & Consultation for a safer digital future	**53**
Technology and Privacy: foresight, oversight and digital transformation	**78**
Artificial Intelligence: preparing for the EDPS's future	**98**
Communicating with impact on data protection	**101**
Celebrating the EDPS' 20th Anniversary	**111**
Human Resources, Budget and Administration	**116**
Governance and Internal Compliance	**125**
Transparency and Access to Documents	**127**
The EDPS' Data Protection Officer	**129**



Foreword

I have the pleasure of introducing you to the EDPS Annual Report 2024 - a special edition as it concludes the EDPS' Mandate 2020 - 2024 and our 20th Anniversary celebrations.

This year has therefore been an opportunity to take stock of the work completed during the mandate, guided by our three-pillar principles: Foresight - Action - Solidarity; to anticipate technologies' benefits and challenges that lie ahead, to provide the necessary tools and take efficient actions to data protection matters, and to ensure that people's privacy is protected according to EU values.

As was highlighted during the EDPS Summit: Rethinking data in a democratic society held in June 2024, the way personal data is processed and the digital landscape as a whole has considerable evolved, and its machinery in constant movement.

Understanding this continuous digital grind, composed of positive and more challenging aspects, the EDPS invested this year in its preparations for Artificial Intelligence's (AI) development and use in EU institutions, bodies, offices and agencies (EUIs).

Ahead of our newly acquired roles under the AI Act as competent market surveillance authority for the supervision of AI systems and notified body for assessing the conformity of certain high-risks AI systems, the EDPS launched its AI Strategy in May 2024. It is based on three key pillars: governance, risk management and supervision. The EDPS also created its very own AI Unit, composed of various experts. Now at the end of 2024, we have put this strategy into motion. We have set up a functioning AI Correspondents Network, including diverse specialists from across the EUIs to foster a collaborative and consistent approach to the use of AI, fostering AI literacy, public procurement and pilot programmes for sustainable and fair EU-centric AI tools, and published guidelines for EUIs on this topic.

Foresight, anticipating technologies and the digital landscape's waves, was also reflected in other areas of our work throughout the year.

With our Technology and Privacy Unit, we pursued our monitoring of technologies' evolution, notably neurodata, and different AI-led technologies, such as retrieval-augmented generation, on-device AI, machine unlearning and plenty others.

Our aim, in this line of work, is to always highlight the possibilities, limits and risks (some of which are unknown - inevitably) of technologies to individuals' personal data and privacy. On that basis, the way data protection by default and by design is embedded in their lifecycle, we steer, with our influence in international fora and platforms, like the Internet Privacy Engineering Network, or the International Working Group on Data Protection and Technology.

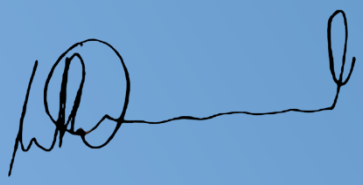
From a Policy and Consultation perspective - another of the EDPS' key areas, and Unit, in which it operates, we provided advice to the EU co-legislator on the Digital Rulebook, which encompasses the AI Act, the Digital Wallets draft Regulations, regulations on the use of health technology. These examples of topics we have worked on demonstrate the direct impact our work has on EU citizens' day-to-day life and their information security and privacy.

Building a safer digital future starts today. With the EDPS' Supervision and Enforcement Unit, we doubled-down on providing essential tools to EUIs, either in the form of Supervisory Opinions, verifying and authorising transfers of personal data to non-EU/EEA countries, training sessions, DPO networking, to ensure that they comply with EU data protection laws for now and the future.

We encourage them to build and share privacy habits - in other words to lead by example in data protection.

Collaboration is a loyal ally to consistent application of EU data protection rules, and their elevation to global standards. With this in mind, we steadily worked with the European Data Protection Board, of which we are a member and provider of its Secretariat, on EU-wide data protection and privacy preoccupations. We led multiple discussions advancing privacy with our participation in multilateral fora, such as the G7 roundtable of data protection and privacy authorities, and the International Organisations workshops we co-organise annually.

We can't predict the future, but we can use our resources, human intelligence and expertise, to prepare for the diverse possibilities and risks that the digital landscape presents.



Wojciech Wiewiórowski
European Data Protection Supervisor

CHAPTER ONE

Presenting the EDPS



1.1.
The EDPS

1.1.1.
Who we are

The European Data Protection Supervisor (EDPS) is the European Union's independent data protection authority responsible for supervising the processing of personal data by the European institutions, bodies, offices and agencies (EUIs). We advise EUIs on new legislative proposals and initiatives related to the protection of personal data. We monitor the impact of new technologies on data protection and cooperate with supervisory authorities to ensure the consistent enforcement of EU data protection rules.



1.1.2.
Our mission

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

Our values and principles

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

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

1.1.3. What we do



We have five main fields of work.

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

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

1.1.4.
Our Powers

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

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

We also have specific powers to supervise the way the following EU bodies, offices and agencies process personal data:

- Europol - the EU Agency for Law Enforcement Cooperation under Regulation 2016/794.
- Eurojust - the EU Agency for Criminal Justice Cooperation under Regulation 2018/1727.
- EPPO - the European Public Prosecutor's Office under Regulation (EU) 2017/1939.
- Frontex - the European Border and Coast Guard under Regulation (EU) 2019/1896.

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



1.2.
EDPS Strategy 2020 – 2024

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

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

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

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

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

CHAPTER TWO

Highlights of 2024



As the 2020 - 2024 mandate ends, we continued to deliver on our actions to shape a safer digital future, operating in our core areas of expertise: **Supervision & Enforcement, Policy & Consultation, Technology & Privacy** and more recently, **Artificial Intelligence**.

In the area of **Supervision & Enforcement**, we:

- **advised EUIs on planned data processing operations in the form of Supervisory Opinions** on transfers of personal data, individuals' privacy rights, data retention and the processing of special categories of data, for example;
- **investigated alleged breaches of data protection laws by EUIs**, such as the European Commission's use of Microsoft tools, or EUIs' use of profiling and automated-decision making;
- **audited EUIs to identify strengths and weaknesses in their data protection practices**, for example in the area of recruitment, the processing of health data and the processing of children´s data for research purposes;
- **addressed complaints from individuals** who believe that an EUI has infringed their data protection rights, including in the context of remote recruitment testing, micro-targeting of social media campaigns;
- **defended privacy and the EDPS' institutional role and decisions before the Court of Justice of the European Union**;
- **collaborated with Data Protection Officers of EUIs to uphold consistent and coherent data protection standards** across EU public administration with the organisation of workshops, trainings, roundtables and various meetings;
- **completed supervisory work in three key areas: Artificial Intelligence, International transfers of personal data** and **collaborating with EU data protection authorities**.

In the area of **Policy & Consultation**, we:

- **issued 97 responses to legislative consultation requests from the European Commission in the form of Opinions, Formal and Informal Comments, providing advice on the data protection implications of draft EU laws and international agreements** on a range of topics, including Justice and Home Affairs, the Digital Rulebook, Artificial Intelligence, international law enforcement agreements, Large- scale IT systems, health, transport;
- **actively contributed to promoting and further developing consistent and coherent data protection rules and practices across the EU**, in particular through our membership in the European Data Protection Board;
- **fostered international cooperation to promote high global EU data protection standards**, for instance at the G7 of Data Protection and Privacy Authorities or at the Global Privacy Assembly.

In the area of **Technology & Privacy**, we:

- **forecasted and analysed digital and technological developments**, highlighting their opportunities and risks in our publications and podcasts of TechSonar and TechDispatch, with a focus on AI and pervasive trends, such as neurotechnologies;
- **organised our Internet Privacy Engineering Network (IPEN)** on automated decision making;
- **helped EUIs address, overcome and prevent data breaches**, and creating awareness campaigns and initiatives;
- **audited IT systems of EUIs**, from websites, to Large Scale Information Systems, such as the Schengen and Visa Information Systems;
- **pursued our actions for digital transformation**, such as updating the Website Evidence Collector and streamlining the organisation of our IT support;
- **prepared for the EDPS' evolving role in cybersecurity** with the Cybersecurity Regulation 2023/2841 and to **improve the preparedness of the EDPS in this area**.

Supporting **internal governance mechanisms and compliance** involved:

- **acquiring legally compliant electronic qualified signatures**, as a further building block the **digitisation** of our processes;
- **creating an ISO-based corporate template for drafting procedures**, ensuring consistency and robustness in EDPS processes;
- **handling 53 requests for access to documents**, the highest number so far and a sign of the growing interest in EDPS activities;
- **the DPO providing independent advice** to internal services, as delegated controllers, with a view to ensure the EDPS' accountability.

Concerning **AI preparedness**, we:

- **created the AI Unit** to take on the EDPS' new tasks under the AI Act;
- **designed and unveiled our AI Act Strategy** based on governance, risk management and Supervision;
- **brought together an AI Act correspondent network of EUIs**.

Communicating data protection involved:

- **communicating on the EDPS' 20th anniversary**;
- **diversifying our online presence** using different tools, mediums and campaigns;
- **leading events to increase visibility of our work** to raise global data protection standards;
- **building and maintaining relationships with journalists**, stakeholders and the public.

As a **working organisation**, we:

- **managed human and financial resources** in a sustainable way to deliver our mandate and tasks;
- **invested in employees, Units and Sectors** by offering trainings on AI;
- **supported the creation of the AI Unit.**

2.1.
Key Performance Indicators 2024

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

The KPI scoreboard contains a brief description of each KPI and the results on 31 December 2024. These results are measured against initial targets, or against the results of the previous year that are used as an indicator.

In 2024, we met or surpassed the targets set in all KPIs, except one, confirming the positive trend of achieving our strategic objectives throughout the year.

One KPI did not fully meet the set target, KPI7, concerning followers EDPS social media account. In particular, in 2024 we continued observing a drop in the number of followers on our X account (ex-Twitter), likely resulting from a general decline in the number of people active on this social media platform.

KEY PERFORMANCE INDICATORS		**RESULTS 31.12.2024**	**TARGET 2024**
KPI 1  Internal Indicator	Cases, incl. publications, on **technology monitoring and promoting technologies** to enhance privacy and data protection organised or co-organised by the EDPS	10 cases	5 cases
KPI 2  Internal & External Indicator	Activities focused on **cross disciplinary policy solutions** (internal & external)	8 activities	8 activities

KEY PERFORMANCE INDICATORS		RESULTS 31.12.2024	TARGET 2024
KPI 3  Internal Indicator	Cases dealt with in the context of **international cooperation** (GPA, CoE, OECD, GPEN, IWGDPT, Spring Conference, international organisations) on which the EDPS has provided a substantial written contribution	39 cases	10 cases
KPI 4  External Indicator	Files on 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
KPI 5  External Indicator	**Article 42 Opinions and Joint EDPS-EDPB Opinions** issued in response to the European Commission's legislative consultation requests	25 opinions	25 opinions
KPI 6  External Indicator	Number of **audits/visits** carried out physically or remotely	10 audits/visits	5 audit/visits
KPI 7  External Indicator	Number of followers on EDPS **social media** accounts	X: 28,860 LinkedIn: 82,881 YouTube: 3409 Instagram: 314	Previous year's figures + 10%
KPI 8  Internal Indicator	Occupancy rate of **establishment plan**	98,8%	90%
KPI 9  Internal Indicator	**Budget** implementation	96%	90%

CHAPTER THREE

Supervision & Enforcement: consistent data protection in EU institutions



One of our core tasks is to supervise the way all EU institutions, bodies, offices and agencies (EUIs) process individuals' personal data, to ensure their compliance with the applicable data protection law, in particular Regulation (EU) 2018/1725, also known as the EUDPR.

This task is carried out by the **EDPS' Supervision and Enforcement Unit**.

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

We also have specific powers to supervise the way the following bodies, offices and agencies process personal data:

- Europol - the EU Agency for Law Enforcement Cooperation under Regulation (EU) 2016/794;
- Eurojust - the EU Agency for Criminal Justice Cooperation under Regulation (EU) 2018/1727;
- EPPO - the European Public Prosecutor's Office under Regulation (EU) 2017/1939;
- Frontex - the European Border and Coast Guard under Regulation (EU) 2019/1896;

This includes:

- issuing Supervisory Opinions, in which we provide advice to EUIs on their planned data processing operations;
- carrying out audits to verify their compliance as well as conducting investigations, following either an alleged infringement or complaint, or on its own initiative;

- cooperate with the Data Protection Officers of the EUIs to promote a strong data protection culture.

Part of the Supervision and Enforcement Unit's work is dedicated to monitoring and supervising the Area of Freedom, Security and Justice, which involves issues related to people on the move, EU and external borders, judicial and law enforcement cooperation between EU Member States, to name a few examples.

Progress Delivered

As supervisor and enforcer of data protection rules for EUIs, we provide them with the necessary tools, guidance and training to ensure that people's personal data is protected.

To achieve this, we:

- **issued Supervisory Opinions** on topics like transfers of personal data, data retention, use of biometric data and data protection concerns linked to the use of AI systems;
- **investigated and audited** the way EUIs process personal data;
- **supervised the area of freedom, security and justice**.

3.1. Supervisory Opinions

Supervisory Opinions provide guidance on complex data processing, ensuring individuals' privacy rights and responsible governance. They are issued either on the European Data Protection Supervisor (EDPS) initiative or at the request of a European Union institution, body, office, or agency (EUIs). In 2024, our Supervisory Opinions addressed several topics, such as data transmission, retention policies, and processing of biometric data.



3.1.1.
Transfers and exchanges of personal data

Ensuring Data Transfers are justified

We provided in January 2024 advice to an EUI **on whether to transmit personal data on request of EU Member States' intelligence authorities**.

In our Opinion, we recommended that EUIs ask EU Member States' intelligence authorities to justify their requests for personal data by providing the reasons why they wish to receive this information, including why this is necessary.

These reasons should also be assessed by EUIs, such as whether providing access to certain data is proportional in light of the objectives pursued and the impact on individuals. EUIs should also consider whether and how to limit the amount of data communicated to EU Member States' intelligence authorities.

We based our advice on the conditions for transmitting data to recipients other than EUIs according to Article 9 of Regulation (EU) 2018/1725, the data protection Regulation for EUIs, and on Protocol (No 7) on the privileges and immunities of the European Union, which governs some of the rules for EUIs.

Read Supervisory Opinion

The exchange of digital social security information

In February 2024, we **issued a Supervisory Opinion on the envisaged integration of the Payment Management Office (PMO) within the Electronic Exchange of Social Security Information System (EESSI)**.

The EESSI is a decentralised system that facilitates cross-border exchanges of personal data on social security benefits. This system is used by 32 participating countries from the EU, the European Economic Area (EEA), Switzerland, and the United Kingdom. The PMO, an internal department of the European Commission, handles the financial entitlements of European Commission staff and other EU institutions.

The Opinion identifies three key points.

First, the transmission of data by PMO is deemed necessary to carry out a task that serves the public interest, supporting digital transformation efforts to ensure that data flows are maintained to provide timely and accurate social security benefits information across borders.

Second, we found that the legal basis proposed by the European Commission for data exchange is insufficient for the PMO's direct handling of social security data. In simple terms, while data sharing is essential, the current justification does not meet the standards required for the processing of such sensitive data. We therefore called for a more robust legal foundation to protect personal data while enabling the necessary data exchanges.

Third, the Opinion highlights a potential shift in the European Commission's role. If, under the new system, the European Commission was to become a user of the EESSI tool, such as taking care of its governance, they would assume the role of a data controller rather than remaining as data processor. This change would entail greater responsibilities for the European Commission in ensuring data protection and accountability.

Read Supervisory Opinion

3.1.2.
How long should data be kept and stored?



Retention period of researchers' personal data

On 1 August 2024, **we issued a Supervisory Opinion on the retention periods for personal data in the context of research**.

The European Research Executive Agency (REA) requested an extension of the current retention periods of personal data of Marie Skłodowska-Curie Actions (MSCA) candidates and funded researchers for historical, scientific, statistical research, and to detect plagiarism and other scientific misconduct.

We therefore issued a Supervisory Opinion on this matter on 1 August 2024, with three important recommendations.

Firstly, we advised that REA uses anonymisation or pseudonymisation techniques if possible, when personal data is further processed for statistical, historical, or scientific research, REA should minimise data exposure. This approach helps protect individuals' privacy by ensuring that only the necessary data is kept, and that sensitive information is not exposed unnecessarily.

REA should also establish a dedicated policy for reviewing its retention practices and access to personal data. This policy should include regular reviews to verify that only data with genuine historical or research value is retained. We recommended the application of strong safeguards, such as a secure database with restricted access. These measures ensure that any extended retention for detecting plagiarism or misconduct is managed securely and transparently.

We found that retaining personal data indefinitely for historical research is not justified. Instead, REA should adopt a specific, extended – but not indefinite – retention period. Regular reviews must be conducted to ensure that only data with continuing historical value is preserved. Additionally, for scientific and statistical purposes, REA should critically assess the necessity of a longer retention period and consider limiting it, if possible, while maintaining the appropriate safeguards.

These recommendations aim to balance the need for long-term research with the fundamental rights of individuals.

Read Supervisory Opinion

Retention policies for EU institutions

On 17 October 2024, the EDPS issued a **Supervisory Opinion concerning an internal Decision adopted by Europol** laying down rules to determine the time limits for the storage of administrative personal data.

The Opinion includes 32 recommendations relevant for all EU institutions when developing internal retention periods applicable to personal data processed by them.

One of the key recommendations included in the Opinion concerns the storage limitation principle, and the need to include the criteria and elements (including possible legal obligations) justifying each retention period within a retention schedule.

In its Opinion, the EDPS also recommends that a documented assessment should always be conducted, detailing the criteria followed to determine the retention periods for each category of personal data processed.

The EDPS also makes several recommendations regarding specific retention periods. For example, the EDPS recommends that:

- a distinction should be made between the different processing activities related to the monitoring of data protection compliance;
- certain retention periods should be adapted;
- the starting date or the activity/event determining the start of the retention period should be clarified.

Read EDPS Opinion issued here

3.1.3.
Other important Supervisory Opinions

Biometrics for MEPs' Attendance



This **Supervisory Opinion examines the European Parliament's plan to introduce a voluntary biometric registration system to record Members of European Parliament (MEPs) attendance in the central attendance registry during a 2-year transitional period**. MEPs can choose between a traditional badge-based system and an optional fingerprint scanning method. Our Opinion, issued on 5 December 2024, focused on establishing a clear and fair legal basis for processing biometric data during this transition.

We found that using consent is the most appropriate legal ground during this period. This means that MEPs must actively agree to have their fingerprints scanned and stored securely using state-of-the-art encryption. Importantly, if an MEP withdraws consent, the system must cease processing their biometric data immediately.

We recommended that the European Parliament rely solely on MEPs' consent for processing biometric data during the transitional period. This avoids any mix-up with other legal bases and ensures fairness and legal certainty for MEPs.

We advised that the amendment to the regulation of MEPs' attendance should explicitly state that biometric registration applies only to the central attendance registry. This clarification helps MEPs understand exactly when and how their biometric data is used.

The European Parliament should make the proposed amendment and the accompanying Bureau Notice widely accessible. For instance, publishing these documents on the European Parliament's website, its social media channels, and in the Official Journal of the European Union to ensure transparency and ease of reference for both MEPs and the public. This will ensure the accessibility of internal rules.

Read Supervisory Opinion

Use of private phone numbers for urgent communication

On 6 November 2024, **we issued a Supervisory Opinion on the use of staff members' mobile phone numbers for urgent internal communication**.

The draft decision proposes that the European Commission may contact staff on security and safety matters, business continuity, and work-related emergencies. While recognising the necessity of ensuring effective communication, we evaluated the data protection implications of using private mobile numbers.

Three key recommendations were issued to ensure compliance with data protection principles:

- we emphasised the need to clarify the definition of "emergency", to help ensure that contacting staff on their private mobile numbers is justified and respects their right to disconnect;
- we suggested limiting communications to corporate devices to help reduce privacy risks while maintaining efficient internal communication. This would prevent the need to process private phone numbers unnecessarily;
- we stressed that once an employee leaves the service, their private phone number should be deleted to avoid unnecessary data retention. This aligns with the data minimisation principles under EU data protection law.

This Opinion highlights the importance of balancing operational needs with employees' privacy rights. By following these recommendations, the European Commission can ensure that staff communications remain efficient, proportionate, and privacy conscious.

Read Supervisory Opinion

3.2. Prior Consultation

Before launching new data processing operations, EUIs must consult the EDPS if these involve high risks to individuals' rights. Through **prior consultations, we assess compliance with data protection rules and provide recommendations to mitigate risks before processing operations start**. If a Data Protection Impact Assessment (DPIA) indicates that risks remain high despite the planned use of safeguards, a preventive consultation with the EDPS is required according to Articles 40 and 90 of Regulation 2018/1725 on administrative and operational personal data.

In addition, Article 39 of Regulation 2016/794 on Europol provides for an ad hoc prior consultation mechanism for new types of processing of operational data, namely data processed by Europol to support EU Member States in preventing and combating serious crime and terrorism.

Similarly, Article 72 of Regulation 2017/1939 on the European Public Prosecutor Office (EPPO) provides a specific prior consultation mechanism for the processing of operational data, namely data processed in the context of criminal investigations and prosecutions undertaken by the EPPO.

Analysing data for medicine safety

In June 2024, **the European Medicines Agency (EMA) requested a prior consultation from the EDPS regarding a DPIA for its EudraVigilance Signal and Safety Analytics Platform (EV SSAP)**. The EV SSAP is designed to enhance pharmacovigilance analytics by managing data on adverse reactions to medicinal products, thus contributing to medicine safety monitoring throughout the EU.

We reviewed EMA's proposed mitigating measures to address high-risk data protection issues identified in the DPIA. We concluded that EMA's proposed measures are sufficient to address identified risks, providing that specific recommendations are followed.

Firstly, we emphasised transparency. EMA should ensure clear and timely communication to individuals whose personal data is processed when changes are made by the EV SSAP, specifying as well the nature of data processing, and its potential impacts via accessible communication channels, providing comprehensive online notices, and collaborating with other data controllers to ensure consistent transparency.

Secondly, security measures must be established. EMA is required to apply strict security measures and, together with its processor, must establish clear procedures to detect and manage security incidents swiftly and effectively.

Thirdly, we highlighted accountability regarding the use of cloud services and international data transfers involving sub-processors. EMA must perform detailed assessments of all sub-processors involved, clearly identifying and evaluating the risks associated with each, especially regarding transfers of personal data outside the EU/EEA. Comprehensive safeguards and ongoing evaluations are necessary to maintain compliance with EU data protection regulations.

By following these recommendations, EMA can manage and mitigate risks, safeguarding personal data effectively and ensuring compliance with EU data protection standards.

Read Supervisory Opinion

3.3.
Investigations



The EDPS conducts **investigations to assess whether EUIs comply with data protection rules. Investigations are essential to identify compliance risks, ensure accountability of the responsible EUIs, and impose corrective measures when EUIs do not process personal data in line with Regulation (EU) 2018/1725**. A formal investigation may be opened when there is a strong indication of an infringement of data protection rules by an EUI.

In 2024, we examined the processing of personal data in EUIs' use of IT systems, which also involved data transfers outside the EU/EEA, as well as their use of profiling and automated-decision making techniques. These inquiries help ensure that EUIs put in place appropriate safeguards, uphold privacy principles, and protect individuals from potential data misuse.

Through our investigative work, we strengthen compliance, transparency, and trust in the way EUIs handle personal data, reinforcing their responsibility towards data protection and security.

3.3.1.
European Commission's use of Microsoft 365 infringes data protection law

In March 2024, we issued our decision following the investigation into the European Commission's use of Microsoft 365.

In this decision, we focused on the European Commission's compliance with Regulation (EU) 2018/1725 on purpose limitation, international transfers, and unauthorised disclosures of personal data.

Key concerns included the lack of control over of processing of personal data when the European Commission uses Microsoft 365 and the insufficient measures put in place to ensure that personal data are adequately protected both within and outside of the European Economic Area.

We found that the European Commission infringed several key data protection rules when using Microsoft 365 and as a result, we imposed corrective measures.

As such, we:

- ordered the European Commission, effective on 9 December 2024, to suspend all data flows resulting from its use of Microsoft 365 to Microsoft and its affiliates and sub-processors, located in countries outside the EU/EEA not covered by an adequacy decision;

- we ordered the European Commission to bring processing operations resulting from its use of Microsoft 365 into compliance by taking specified actions, by way of contractual provision and other organisational and technical measures, for example;
- we also issued a reprimand to the European Commission.

We considered that the corrective measures we imposed were appropriate, necessary and proportionate in light of the seriousness and duration of the infringements found.

Many of the identified infringements concerned all processing operations carried out by the European Commission, or on its behalf, when using Microsoft 365, and impacted a large number of individuals. Affected individuals include not only all European Commission's staff, but also staff of other EUIs and other individuals whose personal data is processed when the institution carries out its tasks using Microsoft 365.

Our decision took into account the need not to compromise the European Commission's ability to carry out its tasks in the public interest or to exercise official authority vested, and the need to allow appropriate time for them to follow our orders, including the foreseen suspension of relevant data flows, and to bring the processing of data into compliance with Regulation (EU) 2018/1725.

The measures imposed by our decision of 8 March 2024 are without prejudice to any other or further action that the EDPS may undertake.

In December 2024, we started following up on the compliance of the European Commission's use of Microsoft 365.

Under the EDPS' decision of 8 March 2024, the European Commission had until 9 December 2024 to demonstrate its compliance with the two aforementioned EDPS orders. On 6 December 2024, the European Commission submitted to the EDPS a report on their compliance with the Decision. The EDPS is examining the information provided; the final assessment is expected for 2025.



This investigation highlights the critical need for EUIs to exercise full control over personal data processing, particularly when relying on large-scale cloud service providers. We continue to monitor developments and support EUIs in adopting solutions that align with EU data protection rules.

3.3.2.
Processing activities amounting to profiling

In 2024, we closed a pre-investigation on the activities carried out by an EUI concerning the handling of applications for public access to documents.



In particular, we looked into how the EUI detects applicants trying to circumvent a queuing system that the EUI implemented for applications for public access to documents. We found that such activities of the EUI constituted profiling within the meaning of Regulation (EU) 2018/1725.

Consequently, we recommended that the EUI inform individuals whose personal data is processed of the existence of profiling as required by the rules on transparency. The EUI should carry out a thorough assessment on whether a data protection impact assessment is necessary.

Automated decision-making in the selection of trainees by an EUI

In 2024, we also opened a pre-investigation into automated decision-making in the (pre)selection of trainees by an EUI.

We are examining to what extent the EUI carries out solely automated decision-making and whether the conditions for such decision-making are satisfied. Those conditions include putting in place all necessary safeguards as well ensuring that individuals whose personal data is processed are appropriately informed of such decision-making.

This pre-investigation is still ongoing.

3.4.
Data Protection Audits

Audits help identify strengths and weaknesses in data protection practices, ensuring that personal data is processed securely and in line with legal requirements. These assessments include on-site inspections, document reviews, and interviews to gain a comprehensive understanding of each institution's data protection framework. We conduct data protection audits to evaluate whether EUIs comply with Regulation (EU) 2018/1725.

Audits serve a preventive and corrective function by allowing us to provide recommendations aimed at enhancing compliance and accountability. They focus on accountability, data security, risk management, governance structures, and transparency in data processing operations. Following an audit, EUIs receive detailed reports with practical guidance on improving data protection measures.

In 2024, audits covered the processing of data concerning health, personal data retention policies, security measures for processing sensitive information and the processing of minors' personal data. These audits reinforced the importance of effective data protection safeguards within the EU administration, ensuring that institutions mitigate risks, improve governance, and uphold individuals' rights to privacy.

Through systematic monitoring and tailored recommendations, our audits support EUIs in embedding a culture of data protection, strengthening public trust in how personal data is handled within the EU framework.



3.4.1.
Audits in the Field of Recruitment

Ensuring fairness in EPSO's remote testing

In 2023, **we carried out an audit of the European Personnel Selection Office (EPSO) activities to assess data protection risks linked to its use of remotely proctored testing, which involves external service providers**. Given that EPSO manages a large volume of candidate data, it must ensure that its selection methods fully comply with EU data protection standards.

The audit report, issued on 17 January 2024, identified several key concerns.

- EPSO must demonstrate that the use of remote proctoring tools involving the processing of biometric data, i.e. facial recognition, in order to verify the identity of candidates, is strictly necessary for selection procedures and that less intrusive alternatives have been considered.
- EPSO must provide a clear legal basis for the processing of biometric data, as these are special categories of personal data that require extra-safeguards under Regulation (EU) 2018/1725.
- In view of the sensitivity of the data processed, the large number of individuals involved, and the innovative use of technological solutions, EPSO must conduct a data protection impact assessment (DPIA).

EPSO must remain in control of the data processing activities carried out by external service providers on its behalf, ensuring that contractual obligations reflect data protection principles and that privacy-by-design measures are fully embedded. We also recommended concrete improvements, urging EPSO to enhance transparency, strengthen contractual safeguards with service providers, and assess the long-term necessity of remote proctoring.

The audit underscored the importance of privacy-respecting recruitment processes. Given that the selection of new EU officials is the "display window" of the EU for the external world. EPSO, as a public administration in charge of dealing with the personal data of a very large number of candidates, should lead by example and show that EUIs comply with fundamental rights, including privacy and data protection, when it comes to designing new selection processes.

Improving transparency in ECB Recruitment

On 19 November 2024, **we issued the report of the audit we carried out at the European Central Bank (ECB), in which we examined the data protection compliance of its recruitment and talent management platform**, Avature, and its use of pre-recorded interviews for job applicants.

The audit highlighted compliance gaps concerning lawful processing, transparency, and candidate rights.

During the audit, we found that the ECB relied on consent as the legal basis for processing candidate data in Avature and pre-recorded video interviews, without offering alternative application methods. Since applicants had no real choice, we concluded that consent was not a valid legal basis under Regulation (EU) 2018/1725.

We also found that information provided to applicants regarding the use of their personal data did not meet the legal requirements of the Regulation. Candidates were not sufficiently informed about how their data would be processed, stored, and shared.

We issued specific recommendations to rectify compliance issues and instructed the ECB to apply corrective measures within a set timeframe to ensure alignment with EU data protection law.



The findings stress the importance of fair and transparent recruitment processes, ensuring that candidates' personal data is processed lawfully and with full respect for their rights. We will continue to monitor the ECB's progress in following our recommendations.

3.4.2.
Audit in the fields of health and medical

In 2024, **we conducted four audits on the processing of medical data within key EUIs, focusing on data retention, transparency, and security**.

The first set of audits examined the Medical Services of the European Commission, the General Secretariat of the Council of the EU, and the European Parliament. These audits assessed whether these institutions correctly applied retention periods for various medical documents in practice. Given the sensitivity of health data, ensuring proper data retention policies is essential to limit unnecessary storage and uphold data protection principles.

Separately, in May 2024, we audited the medical service of Europol. This audit focused on different data protection aspects, particularly the provision of information to individuals regarding the processing of their personal data, the handling of individuals' requests, and compliance with integrity, confidentiality, and storage limitation principles.

With these audits, we reinforced the importance of compliance in the management of medical data across EU institutions and agencies, ensuring that personal data is handled securely, transparently, and lawfully.

3.4.3.
Other important audits

EDPS audit at the Joint Research Centre

In December 2024, **the EDPS performed an audit at the Joint Research Centre in Seville, Spain, focusing on the compliance of their personal data processing operations involving minors and AI in the context of the Human behaviour and Machine Intelligence (HUMAINT) project**. The goal of the HUMAINT project is to advance the scientific understanding of the impact that AI systems have on human behaviour. In this context, one of the studies of the project examined the impact of Embodied AI (robots) on human cognitive and socio-emotional behaviour, including by analysing Child-robot interaction, under the AI Act.

3.5.
Complaints handling

The EDPS **handles complaints from individuals who believe that EUIs have misused or mishandled their personal data**.

A complaint to the EDPS can only relate to the processing of personal data by an EUI. The processing of personal data by a public or private entity of an EU Member State does not fall under the EDPS' competences.

As the independent data protection authority for EUIs, we investigate complaints, provide guidance, and ensure compliance with the data protection law, in particular Regulation (EU) 2018/1725.

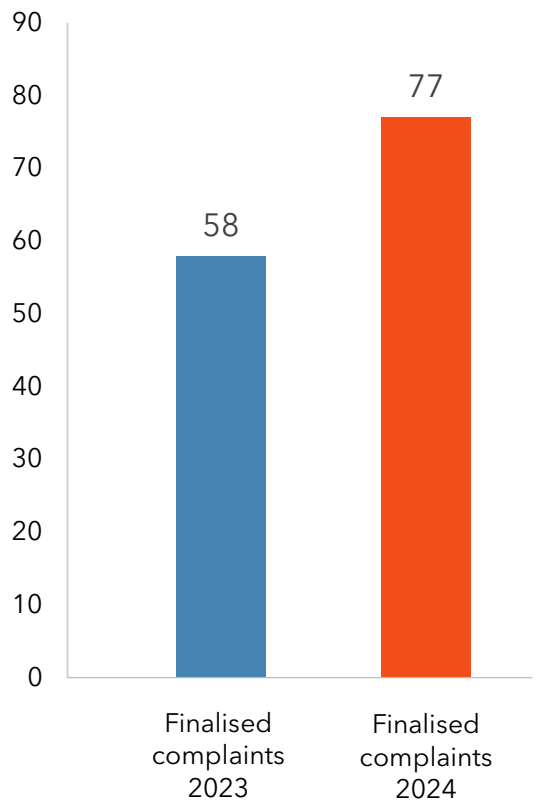
Complaints can be on any unlawful data processing, such as lack of transparency, failure to respect individuals' rights, or inadequate security measures.

Each complaint is carefully assessed, and the relevant EUI is requested to provide clarifications and its views on the alleged infringement. Following the investigation of the complaint, we issue a decision and may impose corrective measures, such as an order to comply with the complainant's rights, or a reprimand, in case a violation of the data protection law is found.

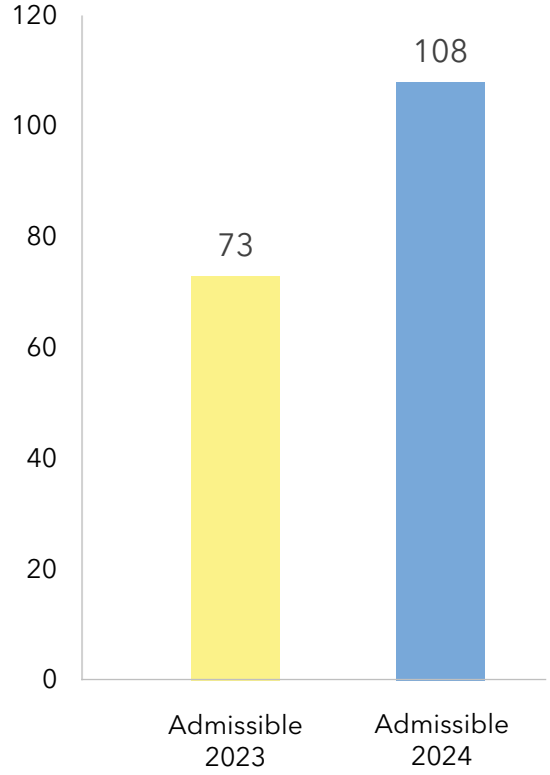
The complaints procedure ensures that individuals' data protection rights are upheld and that EUIs remain accountable for their data processing activities.

In 2024, we handled complaints on, individuals' access rights, unauthorised disclosure, and transparency in data processing practices for example. These cases demonstrate the importance of effective complaint mechanisms in ensuring that individuals can exercise their rights and obtain redress when data protection rules are not followed.

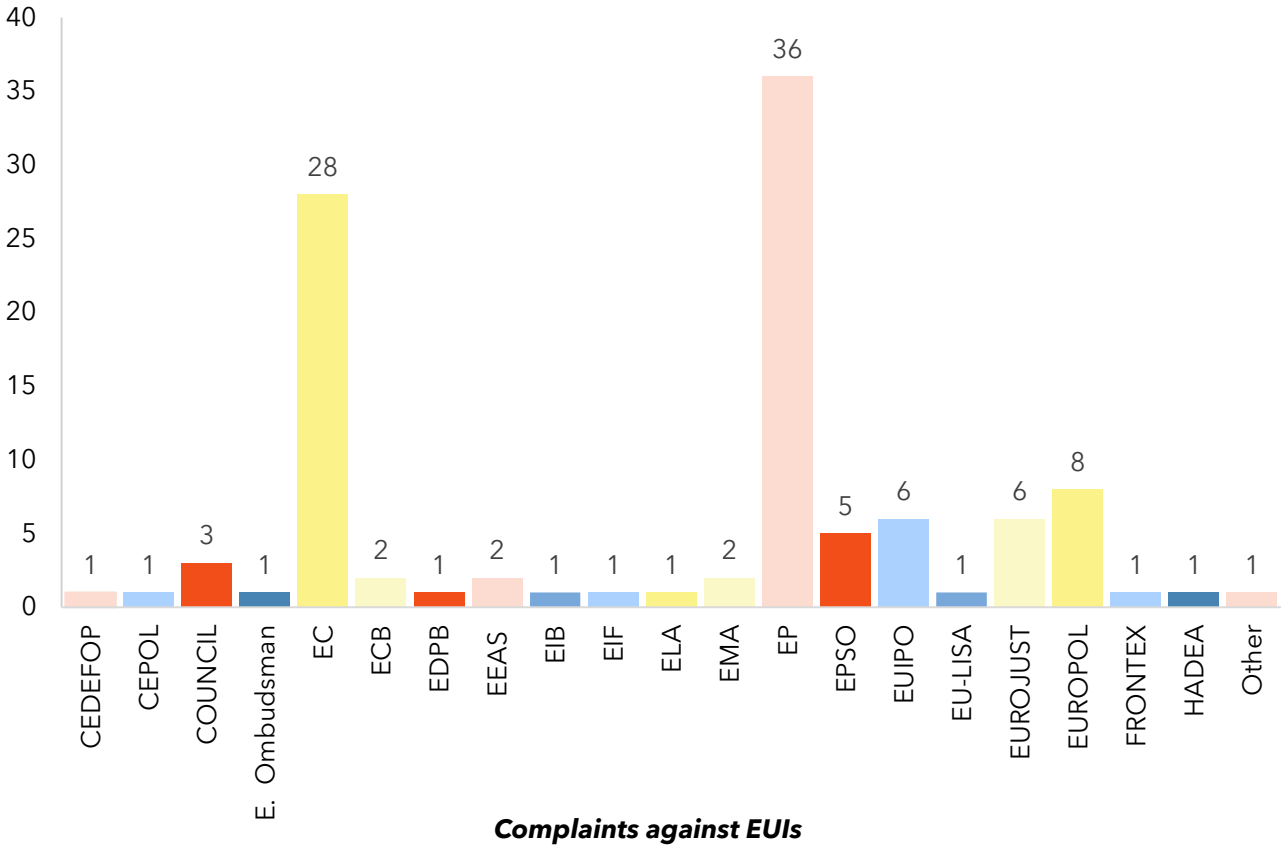
Through our complaint handling, we continue to strengthen compliance, promote best practices, and safeguard the fundamental right to data protection within the EU administration.



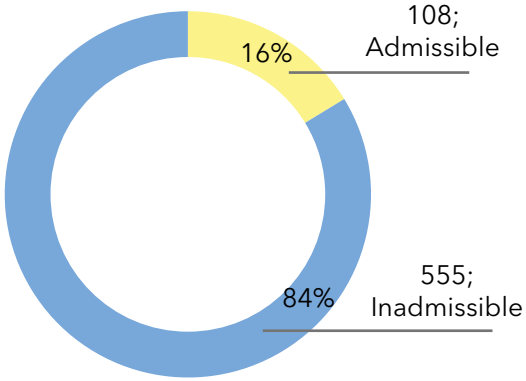
Decisions on complaints



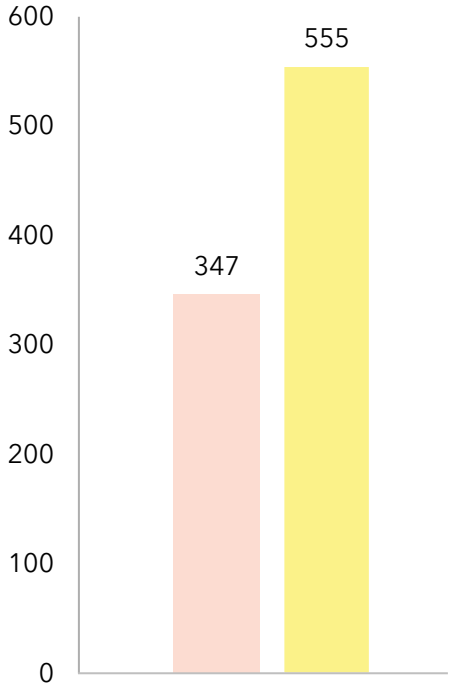
Admissible received 2023 vs 2024



Complaints against EUIs



Admissible/Inadmissible 2024



Inadmissible 2023 vs 2024

3.5.1.
EDPS reprimands EPSO for its remote testing

On 27 November 2024, **we issued a decision on three complaints concerning the European Personnel Selection Office's (EPSO) remote testing used in 2023**.

Amidst COVID-19, EPSO, the main institution in charge of the EU institutions' recruitment procedures, launched remote testing. These online tests involved proctoring subcontracted to an external contractor, whereby candidates were supervised and monitored during the exams.

Assessing the complaints submitted in this context, the EDPS retained most of the allegations made and found that EPSO had infringed certain rules of Regulation (EU) 2018/1725.

Amongst other important findings, we highlighted that:

- EPSO had incorrectly relied on consent as legal basis for processing personal data in the context of remote proctored testing;
- the biometric data of candidates being tested, such as their faces, were processed by EPSO without any legal basis;
- candidates were not provided with fair, transparent and sufficient information about how and for what purposes their personal data were processed;
- these proctored exams were subcontracted by EPSO to another company. EPSO was not in control of the processing operations conducted on its behalf by the subcontractor, which led to transfers of candidates' personal data to non-EU countries, without transfer tools in place to ensure its adequate protection. In the meantime, EPSO terminated the contract with the company in question.

Totalising these observations, the EDPS decided to reprimand EPSO.

Read the Summary of the EDPS Decision on EPSO.

3.5.2.
Issuing a reprimand to the European Commission on its targeted advertising

On 13 December 2024, **the EDPS issued an important decision on a complaint case submitted by a Dutch citizen concerning the European Commission's targeted advertising campaign on the social media platform X, formerly known as Twitter**. The aim of the advertising campaign, which ran on X in September 2023, was to communicate on the Child Sexual Abuse Material (CSAM) legislative proposal.

The complainant, represented by the non-profit organisation NOYB, otherwise known as European Centre for Digital Rights, alleged the unlawful processing of the complainant's personal data in this context.

The EDPS' investigation revealed that the European Commission had targeted X users over the age of 18 from certain EU Member States, including the Netherlands. The campaign also targeted specific X users by including and excluding users that had interacted with posts containing specific keywords set by the European Commission, some of which referred to certain political parties, politicians, Eurosceptic and/or nationalistic political opinions and religious beliefs, as well as targeting users with interests similar to the key accounts selected by the European Commission.

Following these findings, the EDPS found that the European Commission had infringed several provisions of Regulation (EU) 2018/1725, by unlawfully processing the complainant's personal data, including special categories of personal data, such as their political opinions and religious beliefs, without a valid legal basis when targeting them with the advertising campaign.

The European Commission argued that it falls within its activities to inform the public about the content of and the need for legislative proposals, such as CSAM. We found that the European Commission had not demonstrated any valid legal basis to rely on the performance of a task in the public interest or in the exercise of official authority as a ground for lawful processing, We also found that the European Commission had not demonstrated that the conditions for lawful processing of special categories of personal data would be met in the context of the targeted advertising campaign on CSAM.

Taking into account that the processing operation was no longer ongoing, we issued a reprimand.

3.6.
Court Cases

One of the EDPS' tasks is to intervene in cases before the Court of Justice of the European Union (CJEU) and the General Court. There are several ways in which we can be involved in cases before the Court:

- we have the power to refer a matter to the Court;
- our decisions can be challenged before the Court of Justice; and
- we may intervene in cases when these are relevant to EDPS tasks.



Contesting EDPS Decision on the European Commission's use of Microsoft 365

In June 2024, the EDPS was notified that the European Commission and Microsoft had filed legal actions before the General Court of the European Union, contesting the EDPS decision of 8 March 2024, which found that the European Commission's use of Microsoft 365 infringed several key data protection rules (see Section 3.3.1).

The European Commission (Case T-262/24) and Microsoft (Case T-265/24) challenged all aspects of the EDPS' decision, including the findings of infringement and the corrective measures imposed, seeking its annulment.

We fully stand by our decision, and we are actively defending it in court. The European Commission and Microsoft did not request interim measures, meaning that the ongoing legal proceedings do not suspend the implementation of the EDPS' decision of 8 March 2024, which remains fully in force.

Identities in data sharing

On 7 November 2024, the Court of Justice of the European Union (CJEU) held a hearing in Case C-413/23 P (EDPS v. SRB). The case concerns an appeal brought by the EDPS against the General Court's ruling in Case T-557/20, which had sided with the Single Resolution Board (SRB) in a dispute over data protection compliance.

The legal dispute originated from an EDPS decision that found the SRB had infringed Regulation (EU) 2018/1725 by making personal data available to an external consultancy firm during a resolution procedure. The General Court, however, ruled that pseudonymised data shared with another party does not constitute personal data for the recipient, provided that the recipient lacks the means to re-identify individuals.

At the hearing, we argued that this interpretation was legally flawed, emphasising that identifiability must be assessed in an objective manner, considering the specific circumstances of each case. We maintained that data protection rules should apply whenever there is a reasonable possibility of re-identification, even if the recipient does not immediately possess the means to do so.

The Court's judgment on the appeal is expected in 2025.

3.7. DPO Network

At their core, **Data Protection Officers (DPOs) help bridge the gap between data protection law and its practical application. In the EUIs, they are the backbone to achieving data protection compliance**.

Our role is to accompany and advise DPOs on data protection matters, so that, in turn, they can provide independent advice to their respective EUIs to guide them in their compliance with Regulation (EU) 2018/1725.

To this end, we supported and organised various initiatives to elevate compliance with data protection law, throughout the year 2024.

3.7.1. EDPS-DPOs Meeting

In 2024, the EDPS and the DPOs from various EUIs convened for their bi-annual meetings, marking the 54th and 55th sessions of this ongoing collaborative effort. These gatherings serve as a platform for dialogue, cooperation, and knowledge sharing, aiming to ensure consistent compliance with Regulation (EU) 2018/1725 across all EUIs.

The 54th meeting, held on 19 June 2024 in Brussels, was hosted jointly by the European Economic and Social Committee (EESC) and the Committee of the Regions (CoR). This session coincided with the European Data Protection Summit, celebrating the EDPS' 20th anniversary. In his opening address, Supervisor Wojciech Wiewiórowski reflected on two decades of progress in data protection and emphasised the EU's role as a leader in this field.

Discussions that followed highlighted the network's evolution and its role in shaping the current data protection landscape within the EUIs, delving into Artificial Intelligence (AI) systems and their compliance with Regulation (EU) 2018/1725, individuals' access requests, and two initiatives related related to the 20th anniversary of the EDPS: the website compliance scanning and data breach notification awareness campaign.

The 55th meeting took place on 27 November 2024 at the Court of Justice of the European Union in Luxembourg. This meeting featured discussions on storage limitation, and data protection impact assessments, as well as updates on data protection case law and technology monitoring, including insights on emerging A technologies. These discussions showcased the network's commitment to staying abreast of technological advancements and their implications for data protection.

Throughout both meetings, a recurring theme was the importance of collaboration and the exchange of best practices among DPOs to address common challenges. The network continues to play a crucial role in promoting a unified approach to safeguarding personal data across the EU's administrative framework, ensuring that all EUIs adhere to the highest standards of data protection.

3.7.2.
DPO Support Group

The DPO Support Group is a rotating group of around 6-10 DPOs that volunteer to prepare the EDPS-DPOs meeting every year in collaboration with the EDPS' Supervision & Enforcement Unit.

The Group meets every week several months before each EDPS-DPOs meeting.

The Group contributes to preparing the agenda for the EDPS-DPOs meeting and plays an active role in preparing the interactive parts of the meeting, such as workshops and case studies. With their unique experience and insights into the daily work of the EUIs, they provide useful input for the selection of topics to focus on during these meetings.

3.7.3.
DPO roundtables

To further enhance our understanding of the challenges that DPOs experience when applying data protection law in EUIs, the Supervision and Enforcement Unit supports the EDPS' DPO in the organisation of DPO roundtables.

On average 6 to 12 representatives from diverse EUIs participate at a time to these roundtables. For this edition, 14 EUIs were represented.

To ensure fairness and equal representations of EUIs, allowing for a balanced overview of their respective work and impact on data protection to best support them, DPOs apply to participate for the Roundtable on a first come first served basis; priority is given to those who have partaken in less than three meetings.



Topics discussed depend on the relevance and interest these may have for EUIs. This may include, how DPOs deal with transfers of personal data within and outside the EEA, access requests or the use of social media by EUIs.

3.8.
Supervising the Area of Freedom, Security and Justice

As part of our work, we also supervise the data processing operations of the following EU bodies, offices and agencies, which are part of the Area of Freedom Security and Justice (AFSJ):

- the European Union Agency for Law Enforcement Cooperation (Europol);
- the European Union Agency for Criminal Justice Cooperation (Eurojust);
- the European Public Prosecutors' Office (EPPO);
- the European Border and Coast Guard Agency (Frontex);
- the European Union Agency for Asylum (EUAA);
- the European Union Agency for the Operational Management of Large Scale IT Systems in the Area of Freedom, Security and Justice (euLISA).

AFSJ covers a range of policy areas including EU border, asylum and immigration management; police cooperation and fight against crime; and judicial cooperation in civil and criminal matters.

In its 2020-2024 Strategy, we had already identified the challenges posed by the patchwork of measures in police and judicial cooperation and border management for its supervisory and enforcement powers. Nevertheless, in the final year of this mandate, we remained steadfast in our commitment to enforcing data protection rules consistently, in line with applicable EU data protection law, Regulation (EU) 2018/1725, particularly Chapter IX.



This approach is essential to upholding justice, fundamental rights and the rule of law for some of the most vulnerable individuals in a domain where European bodies, offices and agencies' processing powers are wide ranging and carry the risk of serious harms.

We continued supervising AFSJ as a whole, while considering the specificities of each body, office, and agency. Our approach took into account the nature and scope of their data processing operations whenever necessary, ensuring that supervision was both targeted and relevant.

To enhance our supervision work in this field, we also collaborate closely with the Coordinated Supervision Committee operating within the European Data Protection Board (EDPB). The EDPB, of which we are a member, provides us with a platform to strengthen our collaboration with the data protection authorities of the EU in relation to the EDPS supervision of Europol, Eurojust and the EPPO.

In 2024, we focused our supervisory activities over the bodies, offices and agencies in AFSJ around six pillar-actions.

- Preparing for the supervision of the interoperability framework.
- Providing advice on the use of AI tools including machine learning in police and criminal justice cooperation.
- Monitoring new ways of cooperation between Europol and EU Member States in the production of operational analysis.
- Scrutinising the processing of personal data by Frontex from debriefing reports in the context of joint operations.
- Providing advice on the setting up of new systems to process operational personal data by Eurojust (war crime module).
- Reinforcing our cooperation with national data protection authorities through our active participation in the Coordinated Supervisory Committee to coordinate supervisory actions and to further streamline our cooperation in investigating complaints and to provide common advice regarding interoperability framework.

3.8.1.
Preparing for the supervision of the interoperability framework

The EU is setting up **an interoperability framework allowing for the exchange of information between different databases**; currently the Visa Information System (VIS), Schengen Information System (SIS) and European Asylum Dactyloscopic Database (EURODAC).

Three additional databases will be launched in the area of Justice and Home Affairs; that's the Entry-Exit System, the European Travel Information and Authorisation System (ETIAS) and the European Criminal Records Information System - Third Country Nationals (ESCRIS-TCN).

The interoperability framework will introduce technical components to allow the interconnection of these systems and for aggregating data stored in them, as well as advanced biometric identification (e.g. facial recognition) and profiling algorithms for risk assessments.

Despite delays to the roll-out of the interoperability framework in 2024, we continued to prepare the supervision of the extensive processing of personal data these systems will pose, with a focus on monitoring and providing guidance on the development of ETIAS; and deepening cooperation with national Data Protection Authorities for the supervision of data flows through this new data ecosystem.

Providing guidance on the development of ETIAS

There are many **challenges to personal data protection in the supervision of ETIAS**, which we need to monitor from the earliest stages of its development.

ETIAS will process data and support decisions affecting millions of visa-exempt travellers per year; including sensitive information for automated checks against law enforcement databases, watch listing and algorithmic profiling.

The operation of ETIAS encompasses a complex multi-controller framework with shared responsibility between EU Member States and EU agencies, including Frontex, Europol and eu-LISA. In this context, we intensified our cooperation with those ETIAS controllers to provide guidance and ensure compliance with the principle of data protection by design and by default. This included participating in working groups coordinated by Frontex and eu-LISA, as well as flagging data protection concerns to the relevant EU agencies, as well as the European Commission.

Aside from these supervisory tasks, we were an active member of the ETIAS Fundamental Rights Guidance Board, helping develop advice on various aspects of ETIAS implementation, including on how to ensure the right to non-discrimination in the operation of the ETIAS Screening rules and on the right to an effective remedy in ETIAS decisions.

Deepening cooperation with national Data Protection Authorities to supervise interoperability

The **interoperability framework presents challenges for data protection supervision linked to the large volume and complexity of data flows, and multiple controllers, split between EU and national levels**. It calls for stronger, and more coordinated cooperation between the EDPS and national data protection authorities.

In 2024, the EDPS continued to deepen its cooperation with national DPAs, via initiatives in the framework of the Coordinated Supervision Committee (see below, under Coordinated Supervision Committee) which centred in particular on ensuring the correct interpretation and application of provisions to ensure the exercise of individuals'' data protection rights.

We also participated in targeted DPA workshops on interoperability supervision, and organised a roundtable with national DPAs and external legal academics to present the results of a study commissioned by the EDPS to map data flows in the interoperability architecture. The main outcome of the study is a tool allowing to navigate the legal provisions underpinning the interoperability framework was shared with DPAs, with the aim that it will be used to support future supervisory activities.

3.8.2.
Audits of existing Large-Scale IT System



Visa Information System audit

The **EDPS is under a legal obligation to carry out an audit of eu-LISA in the VISA Information System at least every four years, and to audit according to international standards**.

The audit report is then sent to the European Parliament, the Council, the European Commission and to the competent national data protection authorities.

This year, the EDPS VIS audit focused on selected areas of security and data protection of the system following the international standards ISO 27001 and ISO 27002. The audit identified several functional and security-related issues that warrant the attention of eu-LISA's Management and for which we will issue recommendations. The final audit report is expected in 2025.

2024 Updates on Audits

We followed up on the recommendations issued during our 2023 Audit of the Schengen Information System (SIS), the Visa Information System (VIS) and the European Asylum Dactyloscopy Database (EURODAC). We decided to close 21 recommendations during this activity, which were addressed. We will perform in 2025 an additional follow up activity for the remaining recommendations as well as for the recommendations from the EDPS Audit Report 2024 on the SIS.

Coordinated Supervision Committee

Active cooperation with other EU supervisory authorities is particularly important in the AFSJ field, since EUIs exchange an increasing volume of personal data with national authorities, heightening the need for coordinated supervision.

It is also an obligation, under Regulation (EU) 2018/1725 for the EDPS and national data protection authorities to cooperate actively within the scope of their competence for an effective supervision of large-scale IT systems and of the EUIs whenever provided for in EU law.

Cooperation occurs through the Coordinated Supervision Committee (CSC) and the Supervision Coordination Groups (SCGs). The SCGs are expected to be gradually phased out and integrated under the CSC. Our participation in the CSC is thus key to ensure an efficient supervision of personal data flows to and between Europol, eu-LISA, Frontex, Eurojust and EPPO. Participation is also instrumental to supervise efficiently the JHA Interoperability framework.

We played an active role in supporting the activities of the CSC in 2024, including taking over the coordination of the CSC in July 2024 for a two-year term.

As coordinator, we are working closely with the Deputy Coordinators and CSC members to develop new working methods, allowing the CSC to manage efficiently its expanding mandate and tasks. Key initiatives include the establishment of two working groups focused on ETIAS and EES, which will facilitate deeper and more agile cooperation on these specific systems. These working groups will serve as models for targeted cooperation under the new CSC Work Programme 2025-2026.



Adding to our general coordination efforts, we led the development of a guidance note on cooperation methods for handling complaints related to Europol's processing of personal data, which was subsequently adopted by the CSC. To support this effort, we collaborated with national DPAs to create a separate guidance note that clarifies the obligations of supervisory authorities when verifying the lawfulness of national data processing in response to individual's complaint regarding their personal data at Europol. This note also establishes a standardised process to enhance cooperation and efficiency when dealing with Europol-related complaints. Furthermore, we are leading annual coordinated actions to assess the lawfulness and accuracy of Europol's processing of personal data concerning minors under 15 years old who are designated as suspects of crimes and terrorism. These actions involve joint supervision with EU Member States' DPAs to protect the rights of this particularly vulnerable category of persons.

We are also closely monitoring the development of ETIAS, with a focus on interpreting key aspects of the ETIAS Regulation, such as how individuals can assert their data protection rights. As part of this effort, we have been participating in Inter-agency Technical Working Group meetings on ETIAS Data Protection Impact Assessments. Our work in this area has helped identify data protection concerns and challenges related to the ETIAS Regulation, which the CSC highlighted in a letter to the European Commission's Directorate-General for Home Affairs in August 2024.

Participation in Supervision Coordination Groups

In 2024, **we continued to participate actively in several Supervision Coordination Groups (SCGs)**, promoting cooperation and effective oversight of particular large-scale IT systems in the European Union.

SCGs are platforms where Data Protection Authorities coordinate supervisory activities and share best practices on databases and IT systems that are particularly sensitive from a data protection standpoint due to their size, nature, and impact on individuals and their privacy.

Due to the gradual rollout of regulatory updates to these large-scale IT systems, the landscape of mechanisms for supervision cooperation has continued in 2024, with the Coordinated Supervision Committee (CSC) assuming supervision of several extra large-scale IT systems, including the Visa Information System (VIS), previously under the scrutiny of a SCG. Currently, two SCGs remain in operation: one for Eurodac, the European Dactyloscopic system, which supports asylum application management and the prevention of terrorism and serious crime, and another for the Customs Information System.

3.8.3. Europol

In 2024, **we continued to monitor Europol's personal data processing activities to ensure compliance with EU data protection law**.

This year's **supervision of Europol focused on handling datasets, joint operational environments, and the use of biometrics and Artificial Intelligence (AI) tools for example**.

To this end, we:

- issued three Supervisory Opinions on prior consultations related to these topics;
- issued one Supervisory Opinion on the draft model on the Working Arrangement for cooperative relations between Europol and law enforcement authorities of countries outside the EU/EEA;
- issued the report on the inspection carried out in October 2023 together with national authorities, detailed below.

Report on Europol's Annual Inspection

In October 2023, the EDPS conducted an in-depth inspection at Europol 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.

Similar to previous inspections, we invited experts from EU Member States' DPAs to join our inspection since EU countries are Europol's main information providers. As such, the participation of national experts in the inspection process helps raise awareness of any problems arising at Europol level that might have originally occurred at national level and how these can be addressed. For the inspection held in 2023, two experts from the DPAs of Poland and Lithuania participated in our inspection.

The report on that inspection was issued in July 2024. We found a number of shortcomings, which led us to issue **23 recommendations** to ensure or to improve Europol's compliance with the data protection legal framework.

Large datasets

Europol increasingly receives large and complex datasets. These large volumes of data collected often come from diverse sources and may include vast amounts of personal data, including information from seized hard drives and mobile devices. **Analysing and categorising every piece of data within these large datasets is a monumental task**. Recognising these challenges, the EU co-legislators established in 2022 an exceptional regime within the Europol Regulation—specifically Articles 18a and 18(6a). This regime allows Europol to process large datasets that cannot comply with the standard data processing requirements due to their volume and complexity. The exceptional regime includes specific conditions and safeguards to prevent misuse of this data, such as stricter oversight, limited retention periods, and clear purposes for data processing.

Monitoring the application of these new provisions is of utmost importance for us as it derogates from the general rule that limits the sharing of personal data with Europol to data about individuals with a clear established linked to an ongoing criminal investigation or criminal intelligence operation as suspects, victims, contacts, associates or witnesses. Upon assessing different files on this topic, we highlighted the importance of distinguishing between data processed under the normal regime of Article 18(2) of the Europol Regulation and data processed under the exceptional regime, as specified in Articles 18a and 18(6a) of the Europol Regulation. Furthermore, we emphasised that Europol should not mix large, undefined datasets with the regular processing framework designed for categorised data because in cases where the composition of datasets is unknown, applying the regular framework becomes problematic and could lead to non-compliance with data protection standards.

Joint operational environments

Since 2023, **we advise Europol on the importance of clearly defining respective data protection responsibilities of different law enforcement authorities involved, together with the agency, in operational analysis related to criminal investigations carried out in joint data processing environments**.

In December 2024, we issued an Opinion in response to Europol's request for prior consultation on a technical tool to apply the concept of Joint Operational Analysis Case (JOAC). The new technical tool will provide EU Member States with direct access to datasets from Europol's Analysis Projects. In particular, it will allow Europol and EU Member States' authorities to carry out joint operational analysis on Europol systems.

In our Opinion, we emphasised the importance of coordinated supervision by national data protection authorities and the EDPS to ensure a consistent approach to supervisory actions.

We also underscored the need for Europol and the competent authorities of the EU Member States participating in any future joint operational analysis case to conclude an arrangement to clearly define, and agree on, their respective roles and duties to secure effective data protection guarantees in the new joint processing environments.

Biometrics

In the field of **biometrics**, we advised the Agency to conduct case-by-case assessments to ensure that the use of biometric data is justified, necessary, and proportionate. We assessed the use of facial recognition of Europol's Image and Video Analysis Solution (IVAS), to aid in investigations of child sexual abuse material. We found that such use of facial recognition is legally allowed under the Europol Regulation; however, it should be ensured that the actual system meets all data protection requirements, and that the system operates in an accurate and bias-free manner concerning individuals.

Artificial Intelligence (AI)

The **increasing development and deployment of AI tools in various fields, including law enforcement, has led us to assess their use by Europol**.



It is clear to us that these tools are designed and used in a manner that ensures they are trustworthy, fair, and free from bias. This is particularly important in the context of law enforcement, where the consequences of inaccurate or biased decisions can be severe and long-lasting.

Whilst we acknowledge the potential benefits that AI tools can bring to law enforcement, such as enhanced efficiency and effectiveness, we strongly advocate for the application of measures to maintain strong data protection standards. One key measure is the separation of large non-categorised data sets from categorised data.

Categorised data refers to information about individuals who have been identified as suspects, victims, witnesses, or associates of a crime; whereas non-categorised data includes information about individuals who do not fit into these categories or whose relationship to a crime is unclear. Mixing these two types of data can lead to false positives, misidentification, and other errors, which can have serious consequences for individuals and communities.

To ensure that data protection measures are effective, strong oversight policies must be put in place and enforced for processes that rely on AI. This includes regular monitoring and evaluation of the AI systems, as well as transparent and accountable decision-making processes.

As a general rule, we strongly advise that AI is used with caution in law enforcement contexts. While AI can be a useful tool for analysing large datasets and identifying patterns, its results and outputs must be considered as statistical probabilities rather than absolute truths.

This means that AI-generated results should be distinguished from accurate data and should not be relied upon as the sole basis for decision-making. Furthermore, the margin of error that AI tools may present must be taken into account, and decisions should be made with a clear understanding of the potential risks and uncertainties involved.

Tools for transfers of personal data

Europol also consulted the EDPS on the revision of their model working arrangement for **transfers of information to non-EU/EEA countries**, including personal data.

In this regard, we issued an opinion stressing that Europol's choice to use a specific transfer tool is without prejudice to the agency's obligation to verify the existence of the pre-conditions required to use such tool, before transfers are carried out; checking whether this arrangement includes appropriate legal measures under the Europol Regulation.

While working arrangements can provide for mechanisms, procedures and technical details on the processing of personal data, they cannot per se provide the legal basis for personal data transfers. In fact, the possibility to use a working arrangement to operate a transfer of personal data depends on the availability of one of the legal instruments established under Article 25 of the Europol Regulation. This is especially important when Europol bases a transfer on derogations, given the exceptional nature of the circumstances required to justify such transfers. In practice, this means that provisions included in a working arrangement to operate transfers of personal data cannot be considered as automatically ensuring the existence of the 'adequate safeguards' which are required under the Europol Regulation to justify a derogation from the agency's general data transfer regime.

In the opinion, we also signalled to Europol that working arrangements could not be used to operate *subsequent* transfers of data to another organisation outside of the arrangement.

We also recommended that in cases where such working arrangements are used to transfer personal data, the signatory parties verify, within a specific time, whether respect of the purpose limitation principle is effectively guaranteed - on a case-by-case basis.

3.8.4.
Processing of personal data at EU borders

Investigating Frontex's exchange of personal data with Europol

In 2024, the EDPS reprimanded Frontex, the European Border and Coast Guard Agency, for not complying with Regulation (EU) 2019/1896 (Frontex Regulation) when transmitting personal data of cross border crimes' suspect to Europol.

This decision closes the investigation we opened on 9 June 2023, following our audit report of 24 May 2023 into Frontex's activities in its joint operations with EU Member States at the EU's external borders.

In this particular context, we found that Frontex was collecting information about suspects of cross-border crime through interviews of individuals intercepted at the EU borders.

This information was then shared automatically with Europol without performing any kind of assessment on whether transmitting this information was strictly necessary as required by Article 90 (2) (a) of Frontex Regulation. Considering the high risks that this implies for individuals reported as suspects, should that information prove unreliable or inaccurate, we decided to open an investigation.

While this constitutes a severe breach of Frontex Regulation, we decided to limit the exercise of our powers to issuing a reprimand because five days after we issued our audit report, Frontex stopped sharing this information with Europol. Furthermore, Frontex is working closely with Europol to define criteria to assess whether the information collected is strictly necessary for Europol to perform its mandate. On that basis, these two parties are establishing detailed rules for the sharing of such information, before the exchanges resume.

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

During our audit in 2022, **we found evidence suggesting that Frontex may have breached the principle of fairness and the allocation of responsibilities for the processing of personal data collected through debriefing interviews conducted by Frontex border guards with individuals intercepted at the EU's external borders**. Frontex uses these interviews to gather information about the person's journey and about other persons suspected of criminal activities.

In particular, the EDPS found that:

- the vulnerability of interviewees and the circumstances and manner in which interviews take place means that the voluntary nature of these interviews cannot be properly ensured;
- information provided to interviewees concerning the use of data collected is incomplete and misleading;
- there are insufficient safeguards to ensure that interviews are only conducted with people in an adequate mental and physical condition;
- there are no procedural safeguards in place taking into account the risk of self-incrimination, and the status of interviewees as detainees.

Frontex is acting as a joint controller for the collection of data through debriefing interviews together with relevant EU Member State national authorities, without having a joint controllership arrangement in place.

Our findings were confirmed by an onsite inspection carried at a migrant reception centre in Lesbos in July 2023.

The extent of those findings, coupled with the severe nature of the breaches they imply and the fact that Frontex has not respected the deadlines we gave to follow our recommendations led us to open an investigation against Frontex.

European Border Surveillance System

On 20 February 2024, we issued an Opinion on the Agency's processing of personal data in the European Border Surveillance System (EUROSUR), a framework for information exchange and cooperation between EU Member States and Frontex to improve situational awareness and increase reaction capability at the external borders.



EUROSUR includes situational pictures of three different categories:

- national situational pictures: information on the situation at the borders of EU Member States;
- European situational pictures: information on the situation at EU external borders;
- specific situational pictures: information on specific operations at the borders.

EUROSUR also includes fusion services, which are satellites and other surveillance tools in the maritime domain and air borders areas.

We also recommended that in cases where such working arrangements are used to transfer personal data, the signatory parties verify, within a specific time, whether respect of the purpose limitation principle is effectively guaranteed - on a case-by-case basis.

3.8.4.
Processing of personal data at EU borders

Investigating Frontex's exchange of personal data with Europol

In 2024, the EDPS reprimanded Frontex, the European Border and Coast Guard Agency, for not complying with Regulation (EU) 2019/1896 (Frontex Reguation) when transmitting personal data of cross border crimes' suspect to Europol.

This decision closes the investigation we opened on 9 June 2023, following our audit report of 24 May 2023 into Frontex's activities in its joint operations with EU Member States at the EU's external borders.

In this particular context, we found that Frontex was collecting information about suspects of cross-border crime through interviews of individuals intercepted at the EU borders.

This information was then shared automatically with Europol without performing any kind of assessment on whether transmitting this information was strictly necessary as required by Article 90 (2) (a) of Frontex Regulation. Considering the high risks that this implies for individuals reported as suspects, should that information prove unreliable or inaccurate, we decided to open an investigation.

While this constitutes a severe breach of Frontex Regulation, we decided to limit the exercise of our powers to issuing a reprimand because five days after we issued our audit report, Frontex stopped sharing this information with Europol. Furthermore, Frontex is working closely with Europol to define criteria to assess whether the information collected is strictly necessary for Europol to perform its mandate. On that basis, these two parties are establishing detailed rules for the sharing of such information, before the exchanges resume.

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

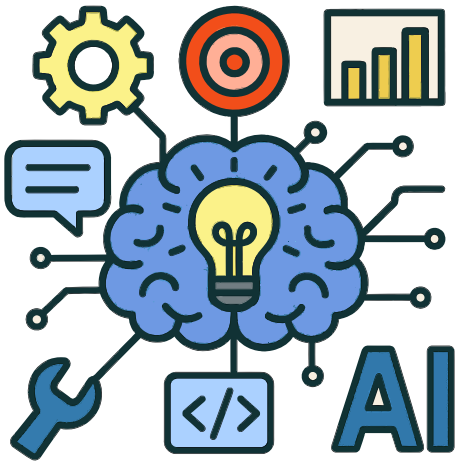
During our audit in 2022, **we found evidence suggesting that Frontex may have breached the principle of fairness and the allocation of responsibilities for the processing of personal data collected through debriefing interviews conducted by Frontex border guards with individuals intercepted at the EU's external borders**. Frontex uses these interviews to gather information about the person's journey and about other persons suspected of criminal activities.

With the evolving role of Eurojust's mandate to preserve, store analyse different forms of crimes against humanity under Regulation (EU) 2022/838, the Agency developed a new database for evidence on core international crimes, the Core International Crimes Evidence Database (CICED).

Since 2022, the EDPS has accompanied Eurojust in its development of the database to ensure its compliance with EU data protection rules. To this end, we have issued three supervisory opinions on CICED: one on the secure transmission of evidence to Eurojust (2022), one on the secure storage of the transmitted evidence (2023), and on the analysis of structured data (2023), focusing on data security and individuals' right of access to their personal data.

On 10 and 11 of June 2024, we carried out an audit at Eurojust premises in The Hague, Netherlands to verify their compliance with data protection law and the Eurojust Regulation when processing operational personal data in CICED. During our audit we also verified if and to what extent our recommendations issued in the context of prior consultations at the first three stages of CICED had been followed.

Consultations: AI-supported translation tools and transfers of personal data



In 2024, we were prior consulted about **machine translation** of evidence in **CICED**.

Our Opinion provides a number of recommendations to ensure that the risks that this tool, supported by AI, are properly and sufficiently identified, and, by extension, that appropriate measures are foreseen and applicable.

We were also consulted on the Joint Investigation Team (JIT) agreements as a tool for transferring operational personal data to non-EU/EEA countries.

In our Supervisory Opinion, we concluded that the proposed data protection clauses of the JIT agreement did not meet the threshold of an international agreement under the Eurojust Regulation. A case-by-case assessment is thus necessary to determine whether the proposed clauses would provide appropriate safeguards for a specific transfer to a non-EU/EEA country.

Whilst we identified areas for improvement, we took positive note of Eurojust's inclusion of essential data protection elements in the model JIT agreement to protect the people's whose data is processed.

3.8.6.
European Public Prosecutor's Office

The European Public Prosecutor's Office (EPPO) is established under Regulation (EU) 2017/1939 (EPPO Regulation) to investigate, prosecute and bring to justice crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud. To fulfil its mandate, EPPO processes operational personal data and is subject to the supervision by the EDPS.

Following up on our 2023 audit recommendations

In 2023, we carried out an audit at EPPO's premises on its compliance with EU data protection law and the Agency's Regulation when processing operational personal data, especially when:

- handling individuals' access requests;
- using the Case Analysis Tool Environment (CATE) - a tool to analyse personal data - on which we also issued a separate Opinion.

We followed up on our 2023 audit during which we had identified eleven formal findings and issued five recommendations to uphold individuals' privacy rights and improve the CATE tool's policy on information storage.

Now in 2024, we found that progress has been made on the application of our recommendations, and that three of our recommendations could be closed so far. Further action on the remaining recommendations will be decided in 2025.

2024	ADVISORY POWERS				INVESTIGATIVE POWERS			CORRECTIVE POWERS
	Opinions on Consultations (formal and informal)	Opinions on Prior Consultations	Audits (carried out and concluded)	Operational visits	Pre-investigations (concluded)	Investigations (concluded)	Complaints (concluded and suspended)	Use of corrective powers
Europol	*1*	*3*	*1*	*1*			*2*	
Eurojust	*2*	*1*	*1*				*1*	
EPPO								
Frontex	*3*				*2*	*1*		*1*
Eu-LISA								
EUAA								
Total AFSJ	*6*	*4*	*2*	*1*	*2*	*1*	*3*	
Total per category	*13*				*6*			*1*

3.9.
Data Protection and AI

Within the **EDPS' role as data protection Supervisor of the EUIs, we guide their use, development and deployment of AI when processing personal data**, by issuing Guidelines, organising training sessions, and providing general advice so that they can embrace the opportunities of these tools, curb their challenges and protect people's privacy at the same time.

3.9.1.
EDPS Guidelines on EU data protection law and Generative AI

We published on 3 June 2024 first guidelines for EUIs to ensure data protection compliance when using Generative AI systems. The guidelines aim to help EUIs comply with the data protection obligations set out in Regulation (EU) 2018/1725, when using or developing generative AI tools.

To ensure their practical application by EUIs, the guidelines emphasise on data protection's core principles, combined with concrete examples, as an aid to anticipate risks, challenges and opportunities of generative AI systems and tools.

As such, the guidelines focus on a series of important topics, including advice on how EUIs can distinguish whether the use of such tools involves the processing of individuals' data; when to conduct a DPIA; and other essential recommendations.

We issued these guidelines within our role as independent DPA of the EUIs, so that they comply with the EU's data protection law applicable to them, in particular Regulation (EU) 2018/1725.

We have not issued these guidelines within our role as AI Supervisor of the EUIs under the EU's Artificial Intelligence Act for which a separate strategy is being prepared.

3.9.2.
Data protection and the use of AI tools by Europol and Eurojust

In the AFSJ, the EDPS issued 3 Supervisory Opinions on the use of AI tools by Europol and Eurojust. (See section 3.8).

3.9.3.
EDPS contribution to the AI Office's consultations

The EDPS contributed to the AI Office's consultation and on the application and defining AI systems and prohibited AI practices under the AI Act.

On 13 November 2024, the European AI Office launched a multi-stakeholder consultation on the application and the defining of an AI system and the prohibition of AI practices, established under the AI Act.

In our contribution, we provided feedback on the definition of 'AI system"; highlighted possible discrepancies of the processing of personal data in the development and deployment of certain AI systems with privacy and data protection law.

This contribution built on the EDPB and EDPS Joint Opinion on the AI Act, as well as relevant EDPB Guidelines, and followed the structure of the questions included in the multi-stakeholder consultation.



3.10.
International Transfers

Model Administrative Arrangement for transfers of personal data

We published the **EDPS Model Administrative Arrangement (Model) for transfers of personal data from EUIs to International Organisations**. The Model aims to help EUIs comply with the applicable EU data protection law, Regulation (EU) 2018/1725, when they need to transfer personal data to International Organisations, within the remit of their role.

Depending on the nature of their work, EUIs may have to transfer personal data to International Organisations to fulfil important objectives, such as providing food assistance or advocating for individuals' rights, for example. In this context, it is one of the institution's priorities to ensure that individuals' personal data is protected according to EU standards both inside and outside the EU/European Economic Area. The new Model Administrative Arrangement allows EUIs to prepare effectively for possible transfers of personal data to International Organisations, in a comprehensive way".

To ensure its practical application by EUIs the Model places emphasis on data protection's core principles and puts in place the necessary safeguards, to ensure a level of protection essentially equivalent to that guaranteed by EU legislation.

As such, the administrative arrangements concluded by EUIs with International Organisations using the model published today will continue to require the EDPS' approval. However, its use by EUIs will greatly facilitate the approval process, to the benefit of both parties and the individuals concerned.

Authorising data sharing with an international organisation

On June 28, 2024, we authorised the use of an amended administrative arrangement between the Single European Sky ATM Research 3 Joint Undertaking (SESAR) and the European Organisation for the Safety of Air Navigation (Eurocontrol). This arrangement facilitates Eurocontrol's non-financial contributions to SESAR, in the context of exchanging personal data necessary for collaborative projects.

Our decision follows a previous temporary authorisation granted in December 2022, which was set to expire on June 30, 2024. In response to recommendations from the initial authorisation, SESAR and Eurocontrol amended their administrative arrangement to enhance data protection measures. We assessed these amendments and concluded that they provide appropriate safeguards for the rights and freedoms of individuals whose personal data is processed involved in the transfers.

We recommended that:

- SESAR and Eurocontrol must clearly define their respective roles as data controllers or data processors to ensure accountability in data processing activities;
- only personal data strictly necessary for the specified purposes should be collected and processed, adhering to the principle of data minimisation;
- both organisations should also improve transparency by providing clear and accessible information to individuals whose personal data is processed about how their data is used, including details on data retention periods and individuals' rights.

We emphasised the importance of following these recommendations to uphold data protection principles and ensure compliance with Regulation (EU) 2018/1725, which governs data processing by EU institutions and bodies.

Our authorisation of the amended administrative arrangement between SESAR and Eurocontrol marks a significant step in facilitating their collaboration while ensuring robust data protection measures are in place. We are committed to overseeing and guiding EU bodies in maintaining high standards of data protection in their operations.

Exceptional transfer tools to share personal data

The European Investment Bank (EIB) requested **the EDPS to authorise transfers of personal data - specifically contact details - to a number of non-EU/EEA countries, including Brazil, Türkiye, India and Fiji, in February 2024**. After assessing these requests, we denied this authorisation because there was not enough evidence and proof that these countries could protect individuals' personal data in the same way as in the EU, otherwise known as an "essentially equivalent level of data protection".

Taking into account the limited and occasional nature of these transfers of personal data, we recommended the EIB to rely on derogations, a type of transfer tool allowing the sharing of personal data outside the EU/EEA on an exceptional basis, on the basis of serving public interest, under EU data protection law.

3.11.
Supervisory cooperation with data protection authorities of the EU/EEA

3.11.1.
Coordinated Enforcement Actions

In 2023 and 2024, we actively participated in **two Coordinated Enforcement Actions (CEF) under the European Data Protection Board (EDPB) framework**.

These actions aim to ensure consistent enforcement of data protection rules across the EEA. The first focused on the role of DPOs, while the second examined how EUIs handle individuals' right of access to their personal data.

Both actions reflect our commitment to ensure that data protection principles are applied effectively in practice and that individuals' rights are upheld.

The role of Data Protection Officers

The first CEF, launched in 2023, assessed how DPOs operate within EUIs.

DPOs serve as key figures in data protection compliance, advising on legal requirements and ensuring that institutions respect individuals' rights when processing personal data. As part of this action, we distributed a questionnaire to DPOs across EUIs to evaluate their role, independence, and ability to influence data protection decisions.

The findings revealed a mixed landscape. While some EUIs fully integrate their DPOs into decision-making processes, others struggle with insufficient resources, unclear mandates and need for additional guidance.

Some DPOs reported that they lacked the authority to challenge non-compliant data processing practices effectively. Others highlighted difficulties in balancing their advisory and oversight functions, particularly in smaller institutions where they often have multiple responsibilities.

To address these challenges, we recommended that EUIs reinforce the independence of DPOs, provide them with adequate staffing and financial support, and ensure that their advice is taken seriously in all data processing decisions. Strengthening the role of DPOs is not just about compliance – it is about fostering a culture of accountability and privacy awareness at all levels of an organisation. The findings of this enforcement action will guide future supervision efforts, ensuring that DPOs are empowered to perform their role effectively.

Ensuring the right of access to personal data

In 2024, the second CEF focused on how EUIs manage individuals' right of access to their personal data. This right is fundamental to transparency, allowing individuals to verify how their data is processed and exercise additional rights, such as rectification or erasure. Despite its importance, many individuals face obstacles when attempting to access their data.

We conducted an in-depth review, analysing complaints and responses from EUIs. The findings highlighted some key findings.

First, most EUIs receive very few access requests - typically fewer than 25 per year - this might be partly due to the existence of self-service tools enabling individuals to download their personal data themselves.

Second, many EUIs rely on decentralised request management systems, leading to inconsistencies demonstrating the compliance in handling the requests.

Third, distinguishing between different types of requests - such as access to personal data versus access to public documents - remains a challenge for some institutions.

Additionally, verifying the identity of requesters often results in excessive data collection, which can paradoxically create new privacy risks.

CHAPTER FOUR

Policy & Consultation for a safer digital future



By acting as an advisor to the EU's co-legislators - the European Commission, the European Parliament and the Council - on all new proposed legislation with impact on individuals' rights to privacy and personal data, we contribute to shaping a safer digital future for the EU and its citizens.

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

In 2024, **the P&C Unit responded to 97 legislative consultations - in the form of Opinions, Formal and Informal Comments**.



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

Our Formal Comments address the data protection implications of Implementing and Delegated Acts and therefore are usually shorter, more targeted and technical.

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

This year we provided our advice across a range of topics, including Justice and Home Affairs, Digital ID and credentials, health technology and medicines assessment, the implementation of the Digital Services Act, etc.

Progress Delivered

In this chapter, find out about **our advisory role** on:

- **justice and home affairs**;
- the **EU's digital rulebook**;
- **health** technology and science;
- as well as our influence in shaping a safer digital future through **international cooperation**.

Evolution of Legislative consultation

The number of requests for legislative consultation has remained very high in 2024. The statistics for 2024 also reflect the continuous expectation of the European Commission's services to involve the EDPS to seek our informal advice at the early stages of preparation of legislative or policy proposals.

4.1. Justice and Home Affairs

Justice and Home Affairs is a specific policy area in which we routinely provide advice and recommendations.

This area regroups matters such as combatting crime, judicial cooperation in criminal and civil matters, management of external borders, asylum and migration, and often involves processing of individuals' personal data, including sensitive information, highlighting the need to protect fundamental rights and freedoms.

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

4.1.1.
Combatting child sexual abuse online

We issued an **Opinion on the proposed Regulation to extend the temporary derogation from certain provisions of the ePrivacy Directive to combat child sexual abuse online**.



The Regulation would allow providers of certain independent interpersonal communication services to continue to apply specific technologies to private communications in order to detect child sexual abuse material for two more years, whilst negotiations for a long-term Regulation are ongoing.

In the Opinion, we expressed concern about the aims of this Regulation, which would, in effect, restrict individuals' fundamental rights to privacy and personal data, including their right to the confidentiality of communications. The EDPS also highlighted that the recommendations previously issued in its Opinion on temporary derogations from the ePrivacy Directive 2020 were not fully addressed, further putting individuals at risk.

Extending the validity of the Regulation on temporary derogations from the ePrivacy Directive is not a formality. It would perpetuate the already-existing risks to individuals' privacy and their personal data, which should by no means become the norm.

We underscored that, although the use of specific technologies to detect child sexual abuse material would remain voluntary, it is still the EU's co-legislators responsibility to put in place measures to ensure that the Regulation complies with the EU's Charter of Fundamental Rights.

In line with previously issued recommendations, we reiterated that the proposed Regulation does not include sufficient and effective safeguards to prevent general and indiscriminate monitoring of private electronic communications. Putting these safeguards in place is important, especially given the high error rates observed with certain technologies used for detecting child sexual abuse materials or child solicitation, such as grooming. We underscored the significant risk that technologies used to detect child sexual abuse material may flag consensually produced and shared imagery.

Whilst we fully support the aim to combat child sexual abuse as a terrible crime, the goal of combatting child sexual abuse must be pursued with the necessary safeguards for individuals' private communications, and, by extension, their fundamental rights to privacy and personal data.

4.1.2.
Europol: preventing, detecting and investigating smuggling of migrants

We published on 23 January 2024 an **Opinion on a Regulation to enhance police cooperation to prevent, detect, and investigate the smuggling of migrants and the trafficking of human beings, and to reinforce the role of the EU Agency for Law Enforcement Cooperation (Europol) in preventing and combating these crimes**.

We made a series of recommendations on four key issues in the proposed Regulation that could have an important impact on individuals' personal data and privacy. This includes the increased processing of biometric data; the role of the European Border and Coast Guard Agency (Frontex) in its cooperation with Europol; transfers of personal data by Europol to countries outside the EU/European Economic Area (EEA); and Europol's support to the competent authorities of the EU Member States. The EDPS' Opinion also takes into account the findings and ongoing work of its supervisory activities regarding Europol and Frontex.

With this Opinion, we aim to strike a balance between helping the EU address illegal migration and keeping individuals and their personal data safe.

The fight against the smuggling of migrants and trafficking of human beings is an important objective of general interest. At the same time, the necessity and proportionality of the proposed measures must be carefully assessed. Therefore, we expressed regret about the lack of an impact assessment; given the nature of the personal data - in this case sensitive biometric data at stake and that vulnerable people - in this case migrants may be involved. We consider that this should not constitute a precedent for any future legislation having comparable impact on the fundamental rights to privacy and data protection.

Detailing our recommendations, we highlight the risks posed by the envisaged increase of the processing of biometric data, including facial recognition, by Europol. In our Opinion, the EDPS' advice is clear: it is necessary to establish mechanisms and clear binding rules that provide appropriate safeguards to mitigate the risks to individuals.

We note that the Regulation plans for a stronger cooperation between Europol and Frontex. In its Opinion, the EDPS submits that the role, limits and procedures to be followed by Frontex when performing its tasks to support Europol and the EU Agency for Criminal Justice Cooperation (Eurojust) and law enforcement authorities of the EU Member States should be clarified. Frontex should not turn into a law enforcement agency, adds the EDPS in its recommendations.

The Regulation provides for transfers of personal data outside the EU/EEA by Europol to be made based on derogations (exemptions) from the general rules on transfers of personal data. In its Opinion, the EDPS warns that the use of such exemptions should not lead to systematic, massive or structural transfers of personal data. In light of this, the EDPS advocates for the use of structural tools for transfers of personal data instead.

In relation to Europol's investigative activities to support EU Member States, we recommend clarifying the responsibilities allocated to the competent authorities in the EU, including defining the type of access to personal data these authorities may have and for what purposes.



4.1.3. International law enforcement agreements

As advisor to the EU co-legislator, we provide our advice on drafted regulation or rules that envisage the transfers of personal data in the field of law enforcement, an area that presents specific risks for individuals and may lead to considerable negative impacts, if their information is mishandled.

EU-Bosnia and EU Lebanon Agreements: enhancing judicial cooperation in criminal matters

We issued two **Opinions on the proposed Agreements between the European Union and Bosnia & Herzegovina, and between the European Union and Republic of Lebanon the cooperation between Eurojust and these countries' competent authorities for judicial cooperation in criminal matters**.

The objective of both Agreements is to enhance judicial cooperation with Eurojust by allowing the Agency to transfer personal data to support and strengthen cooperation in investigating and prosecuting serious crime, in particular organised crime and terrorism, while ensuring appropriate safeguards upholding fundamental rights and freedoms of individuals, including privacy and the protection of personal data.

Recognising the benefits of this cooperation, especially in tackling complex transnational offences, nevertheless data collected and transferred to authorities in Bosnia & Herzegovina and in Lebanon must guarantee the same level of protection that applies in the EU. This includes independent oversight, clear retention periods, strict purpose limitation, transparent rules on data access, and others.

While we concluded that both Agreements provide adequate safeguards to protect individuals' fundamental right to data protection generally, we offered some specific recommendations to facilitate the practical application of the future Agreements, including guidance that may be relevant for future agreements with other countries outside the EU/EEA for which negotiations either are about to begin or are underway.

Our recommendations focused on onward transfers of personal data, the right to erasure of personal data, the possibility to postpone or suspend transfers of personal data and on the review and evaluation of the Agreements.



Read the Opinion on Bosnia & Herzegovina

Read the Opinion on Lebanon

EU-Canada agreement on transfers of Passenger Name Record Data

We issued an **Opinion on the EU-Canada agreement on transfers of Passenger Name Record (PNR) data.** PNR data is information provided by passengers, collected and held by airlines for commercial purposes.

In this Opinion, published on 29 April 2024, we reached the conclusion that the draft Agreement contains the necessary safeguards required for it to be compatible with the Charter of Fundamental Rights.

At the same time, we make several recommendations with the aim to ensure that the future Agreement would be implemented in compliance with EU law. These recommendations focus on:

- the retention of PNR data of departing passengers should be limited and only carried out under certain circumstances;
- any use of PNR data for the purposes of security and border control checks should be possible only when those checks are carried out to prevent, detect, investigate, or prosecute terrorist offenses or serious transnational crime, and not for other purposes such as immigration control for example;
- the access to retained PNR data without prior review by a court or independent administrative body should be allowed only in exceptional and duly justified cases.

We consider that the European Commission should pay special attention to these elements, as well as to the exercise of individuals' data protection rights, during the joint reviews of the envisaged EU-Canada Agreement.

4.1.4.
Large-scale IT systems and interoperability



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

This is an area where the EDPS has continuously been paying special attention in view of the potential impact of the processing of personal data in the systems on a very large number of individuals.

Recommendations: personal data and visa applications

We provided Formal Comments on a proposed European Commission Decision on data entered, stored and accessed in the Visa Information System (VIS). VIS is an EU-wide platform used by national authorities to process and examine visa applications. Its functions range from capturing personal information and links between applications, to generating logs and statistics for monitoring and reporting.

Overall, our stance is that while the system's technical groundwork is designed to help streamline visa processes, these updates must not compromise individuals' privacy rights. Adopting clear definitions, limiting additional access rights to strictly foreseen cases, and citing the legal framework accurately are key to achieving a well-balanced approach.

Amongst our advice, we recommend to:

- clarify references to technical specifications to help users and oversight bodies fully understand the obligations laid down in the Implementing Decision;
- ensure a proper legal basis for any new or temporary access rights granted to entities outside the main VIS scope, including the European Travel Information and Authorisation System of National Units;
- strengthen transparency by referencing the correct legal framework and clearly explaining any changes that affect personal data processing or storage.

Defining security, illegal immigration and high- epidemic risks

We evaluated a proposed **European Commission Decision that revises rules for identifying risks under the European Travel Information and Authorisation System (ETIAS)**. The goal is to align how security, illegal immigration, and high epidemic threats are defined within the Visa Information System (VIS). We raised serious data protection concerns, as the revised Decision removes key safeguards on how risks should be specified and assessed, potentially increasing the risk of arbitrary profiling and excessive data processing.

We warned that the revised Decision replaces detailed criteria for risk assessment with a simplistic list of offences, which mostly duplicates crime categories already in the ETIAS Regulation. Without clear risk definitions and safeguards, there is a high risk of unjustified or discriminatory profiling of travellers, infringing their fundamental rights to privacy and data protection.

We stressed that risk factors must be specific and evidence-based to prevent disproportionate processing of personal data.

To strengthen privacy safeguards, we also call for explicit consultation with the ETIAS Fundamental Rights Guidance Board, which plays a critical role in assessing the impact of risk indicators on fundamental rights, non-discrimination, and personal data protection.

We therefore advised to:

- strengthen risk definitions to prevent excessive and unjustified data collection, avoiding the overbroad categorisation of offences as risk factors;
- reinstate the requirement to remove obsolete risks, ensuring compliance with data accuracy and proportionality principles;
- consult the ETIAS Fundamental Rights Guidance Board to ensure risk indicators do not enable unlawful profiling or violate privacy rights.

SIRENE Manuals: assessing updates and privacy impacts

We **assessed the European Commission's decision to repeal and replace two SIRENE Manuals**.

SIRENE stands for Supplementary Information Request at the National Entries, a mechanism ensuring efficient exchange of information about alerts stored in the Schengen Information System (SIS). These two Manuals provide operational guidelines for national SIRENE Bureaux on topics ranging from border checks and return procedures, to police and judicial cooperation in criminal matters.

In practice, the proposed changes focus mainly on technical and procedural updates. They aim to reflect the adoption of new EU frameworks, in particular the European Travel Information and Authorisation System (ETIAS) and the reformed Visa Information System (VIS). We noted that these modifications are designed to streamline the process of sharing relevant data across Member States while maintaining coherent and speedy communications between SIRENE Bureaux.

Because these Manuals are limited to clarifying existing rules and procedures, we concluded that no new data protection concerns arise. Under the new instructions, national authorities will continue exchanging personal data only insofar as strictly necessary for matters of border management, return operations, police investigations, and judicial cooperation. We emphasise that these measures retain previously established safeguards, meaning individuals' privacy rights remain unaffected.

Read the Formal Comments



4.2.
Digital Travel Credentials and Digital Identity Wallets

We provided advice regarding **the data protection implications of the draft Regulations on the EU's digital identities, wallets and credentials currently under negotiation at EU level**.

Whilst this project aims to bring about an EU-wide approach for individuals to verify their identity and access to services, such as health or banking, it also presents risks for individuals' privacy, requiring robust data protection measures on a legislative and technical level.

Digital travel credentials: a simpler journey

We examined the Council's proposed Regulation on **issuing digital travel credentials based on identity cards**.

This Proposal intends to offer EU citizens a digital version of their identity card that can be used as a travel credential, making border crossings and other free movement processes more straightforward. We welcomed this approach, noting the potential for smoother travel and reduced administrative burdens when EU citizens ascertain their freedom of movement.

We highlighted that digital credentials should be strictly voluntary. Individuals should be able to choose whether they want to use this digital alternative. Under no circumstance should someone who opts out of using digital credentials face discrimination or extra requirements. We also underlined the principle of data minimisation, taking positive note that the proposed Regulation excludes fingerprints from the digital credential. This measure aligns with good privacy practices, ensuring that only necessary data is stored.

We also examined the connection of this proposal with the European Digital Identity Wallet (EDIW), and recommended clarifying precisely how digital travel credentials fit alongside personal identity data already in the EDIW. A well-defined framework should help avoid confusion, prevent duplication of data, and maintain robust data protection.

Whilst we did not flag major data protection concerns at this stage, we outlined three key recommendations:

- to keep issuance voluntary so individuals who do not opt in face no negative consequences;
- to exclude fingerprints to uphold data minimisation and privacy;
- to clarify alignment with the European Digital Identity Wallet, specifying how both systems will interact.

Read the Opinion on digital travel credentials

Enhancing Efficiency of border checks

We reviewed a proposed Regulation on **the application for the electronic submission of travel data, the EU Digital Travel application**. This initiative intends to make crossing borders simpler for travellers while enhancing security. By sending digital versions of travel documents in advance, individuals could save time at the border and help border authorities focus on more pressing security matters.

We noted that this system does not require additional personal data not already processed for borders. Instead, it digitises the same data travellers would otherwise show in person. Submitting this data in advance could speed up border controls, reduce waiting lines, and free up border staff to conduct more targeted checks. However, we stressed that transmitting data remotely means it can be more vulnerable. Strong security measures are therefore vital. These should include robust encryption, strict oversight, and immediate removal of any data once a decision is reached on granting or denying entry.

Travellers should have the option to use or not the system without facing negative consequences. Additionally, we recommended clarifying how digital travel credentials will interact with the European Digital Identity Wallet (EDIW). This will ensure consistent handling of personal information across different EU digital services.

To ensure full compliance with data protection regulations we advise to:

- ensure that data is deleted after entry is granted or refused, unless justified for other legal reasons;
- emphasise that competent border authorities should delete travel data immediately after the traveller has been accepted or after an adequate period;
- clarify the link between digital travel credentials and the European Digital Identity Wallet to maintain consistency.

Read the Opinion on the electronic submission of travel data

Reviewing the rules for the EU Digital Identity Wallets

We published several sets of Formal Comments assessing the proposed rules **to apply the Regulation on governing the European Digital Identity Wallet (EDIW), which allow users to securely store and share their identity for electronic transactions**. All these rules must explicitly align with the EU data protection framework, including the GDPR, applicable in EU Member States and the ePrivacy Directive governing electronic communications. First, we called for stronger data protection by design and default, ensuring that the EU Digital Wallets incorporate privacy-enhancing technologies (PETs) such as pseudonymisation, encryption, and selective data disclosure. This would allow users to share only the necessary information, keeping their full legal identity hidden when possible.

We warned against tracking risks and urged that transactions should remain unlinkable to prevent profiling. Additionally, we recommended strict data minimisation rules, ensuring that revoked identification data is not stored indefinitely and that personal identity records are only accessible when necessary.

Second, we stressed the need for robust security measures and certification requirements. The Regulation should mandate strong security standards, ensure wallet providers notify security breaches in compliance with GDPR, and promote certification schemes that align with EU data protection laws. EU Digital Wallets must also support standardised protocols to facilitate secure and privacy-preserving interactions with service providers while preventing excessive access requests that could expose users to tracking risks.

Third, we support a secure notification and reporting system for EU Member States to register wallet providers and relying parties. This system must use state-of-the-art encryption and access control to prevent unauthorised access to sensitive identity data. Additionally, wallets should allow users to report unlawful data requests, request data erasure, and include automated controls to detect and block excessive data requests.

These recommendations ensure that the EU Digital Identity Wallets remain secure, privacy-friendly, and aligned with EU legal standards, protecting users from excessive data collection, tracking, and security risks.

Read Opinion on the integrity and core functionalities of European Digital Identity Wallet.

Read Opinion on personal identification data and electronic attestations of attributes issued to European Digital Identity Wallets.

Read Opinion on protocols and interfaces to be supported by the European Digital Identity Wallets.

Read Opinion on notifications to the Commission concerning the European Digital Identity Wallet Ecosystem.

4.3.
Health Technology Assessment



The EDPS issued formal comments on several draft implementing regulations pursuant to Regulation (EU) 2021/2282 on health technology assessment. **A health technology assessment summarises information related to the use of a health technology, such as a medicinal product or a medical device**.

The draft implementing regulations provide among others for:

- procedural rules in relation to joint clinical assessments and joint scientific consultations of medicinal products for human use at Union level;
- rules regarding the management of conflicts of interests in the joint work of the Member State Coordination Group on Health Technology Assessment (Coordination Group) and its subgroups; and
- procedural rules for the cooperation of the Coordination Group and the Commission with the European Medicines Agency.

The EDPS welcomed the provisions on data protection, while making recommendations on how to further safeguard the processing of personal data of data subjects involved in health technology assessment. He also recommended clarifying the methods used to identify relevant experts to participate in joint clinical assessments. The EDPS also provided recommendations regarding on the publication of information about experts that participated in the joint work of the Coordination Group and considered that the Commission should further justify the need for such publication and ensure that it complies with the requirements of necessity and proportionality.

Read the Formal Comments in full

4.4.
Implementation of the Digital Services Act

In 2024, we followed up on our Opinion on the Proposal for a Digital Services Act (DSA), providing more specific advice on implementation aspects of this Regulation that aims to create a safer, fairer and more transparent digital space.



Access to data by vetted researchers

Following our Opinion on the EU's Digital Services Act (DSA) Proposal, we closely followed up on its application and practical use by guiding the EU legislator. To this end, we advised the European Commission on their draft Delegated Regulation on the technical conditions and procedures for data sharing by very large online platforms and very large online search engines with vetted researchers under the DSA. With these rules, the aim is to ensure that data access is secure, transparent, and fully compliant with EU data protection rules.

Assessing these rules, we welcomed the strict security and confidentiality requirements envisaged for data sharing with vetted researchers. Applicants must prove they have put in place strong safeguards before gaining access. This ensures that personal data is handled securely and only by those who meet high standards of protection. The rules also require clear procedures to prevent data misuse, reinforcing individual privacy rights.

In particular, we stressed the need for access to data to be proportionate and necessary in light of the goals pursued. Researchers must justify their requests, ensuring that only the minimum data needed for research is shared. If anonymous or pseudonymous data can achieve the same research goal, such data should be used.

We also call for greater clarity on roles and responsibilities. The European Commission's role in the DSA data access portal must be clearly defined because some provisions of the draft delegated Regulation suggest that the European Commission acts as a data processor, while others imply that the European Commission acts as a controller. This distinction is important for legal clarity and accountability.

Read the Formal Comments

4.5.
Participating in EU regulatory bodies and experts groups

In 2024, the EDPS participated in a number of expert groups. We contributed to discussions on emerging challenges and shared our data protection expertise. These forums foster collaboration among institutions, policymakers, and industry stakeholders. Our participation helps shape robust and future proof policies of the EU.

4.5.1.
High-Level Group for the Digital Markets Act

The EDPS is a member of the High-Level Group (HLG) for the Digital Markets Act (DMA), alongside representatives of the EDPB. The HLG's purpose is to provide advice and expertise to the European Commission to ensure that the DMA and other sectorial regulations applicable to gatekeepers are followed in a coherent and complementary manner.

The Group may also provide expertise in market investigations into emerging services and practices.

In 2024, the HLG issued a public statement on Artificial Intelligence that outlined both the promise and the challenges of AI technology. Whilst AI drives innovation and growth, it also presents significant risks—such as bias, data misuse, and threats to fundamental rights. In the statement, the HLG underlined that personal data must be collected, aggregated, processed, and used in ways that are lawful, transparent, and fair, including when used for training AI systems, in full compliance with legislation protecting the right to the protection of personal data and other fundamental rights. You can read the public statement here.

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

4.5.2.
European Data Innovation Board

Alongside the EDPB, we are also a member of the European Data Innovation Board (EDIB). The EDIB is an expert group, chaired by the European Commission, established under the Data Governance Act (DGA), a regulation aiming to provide a framework for trustworthy voluntary data sharing across different fields. The EDIB is set up to support a consistent approach to data governance across the EU, by bringing together regulators and experts to provide guidance on data exchange, standardisation of some of the DGA's rules and collaboration with its different actors.

The EDPS attended 4 meetings of the EDIB and contributed to discussions on the DGA from a data protection perspective.

4.5.3.
High-Level Group on access to data for effective law enforcement

We participated as observer in the High-Level Group on Access to Data for Effective Law Enforcement (HLG), 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.

4.6.
Towards a Digital Clearinghouse 2.0: focus on cross-regulatory cooperation

"Towards a Digital Clearinghouse 2.0" is an initiative (re)developed to promote effective enforcement in the digital world, announced in the context of the EDPS as part of our 20th anniversary celebrations (see chapter 8). Building on our experience with the original Digital Clearinghouse operating from 2017 to 2021, our aim is to enhance cross-regulatory cooperation and to address overlaps of the existing and recently-adopted EU digital rulebook.

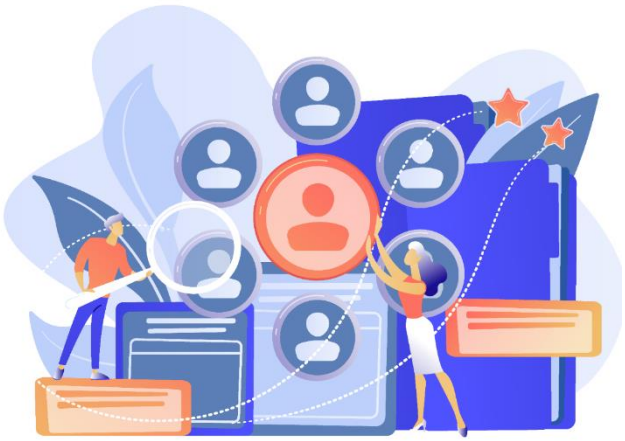
We propose a vision for a common forum for enforcement bodies and regulators to be able to exchange information, share best practices, and coordinate efforts at EU level, in order to consistently apply EU law in a data-driven economy.

Within this process, we organised on 24 October 2024 a seminar to discuss our idea with key stakeholders. The discussions were on shaping the future of digital governance and improve the enforcement of digital rules.

Discussions at the event focused on overcoming current challenges such as disparities in the way current rules for the digital world are applied, their differences, and sometimes overlaps. Participants examined how recent regulatory developments – including the Digital Services Act, Digital Markets Act, Data Governance Act, Data Act, and Artificial Intelligence Act – will impact enforcement practices and regulatory cooperation.

The contributions received during the Seminar informed the concept note that we will publish on this matter in 2025. With this initiative, we call for a coherent, consistent approach to the application of data protection, with other relevant EU laws in the digital sphere. By fostering a coherent application of the EU law, we hope to ensure that digital markets remain fair and transparent while preserving fundamental rights.

4.7.
Cooperating with the European Data Protection Board



As part of our work and responsibilities, we are both a member and provider of the Secretariat of the European Data Protection Board, the independent body in charge of ensuring consistent application the GDPR and the Law Enforcement Directive across EU/EEA countries.

To ensure consistent and impactful involvement of the EDPS as a member of the EDPB, we have set up an internal taskforce to coordinate our involvement and work on EDPB files.

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

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

We also coordinated a taskforce on the cooperation with competition and consumer protection authorities, which is amongst others developing a joint guidance (together with the European Commission) 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 continue to coordinate in 2025.

With our targeted and strategic involvement on certain key EDPB initiatives, we strive to represent the EU perspective, using our expertise as supervisor of EU institutions, to ensure that EDPB considerations are anchored in EU law, including in the case law of the Court of Justice of the EU, and apply the general principles of EU law.

This year, we provided significant contributions to various key EDPB documents adopted in 2024, including:

- 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 Guidelines 01/2023 on Article 37 Law Enforcement Directive, adopted after public consultation on 19 June 2024;
- Guidelines 1/2024 on processing of personal data based on Article 6(1)(f);
- 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 of a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679;
- Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement;
- 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;
- Guidelines 02/2024 on Article 48 of the GDPR; and
- EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.

4.8. Providing secretarial support to Supervision Coordinated Groups

In 2024, we continued to provide the Secretariat, including logistical support, to the Supervision Coordinated Group for the Customs Information System (CIS) and for the Supervision Coordinated Group for Eurodac, both of which are part of the EU's large-scale system in the field of border management. In this context, we assisted the Chairs and Vice-Chairs of these Supervision Coordinated Group in preparing and organising meetings, as well as contributing to discussions on multiple files. More information regarding the SCGs and their activities are published on the respective webpages of the CIS and Eurodac on the relevant EDPS webpage.

4.9.
International Cooperation

We actively foster international cooperation to elevate data protection standards worldwide. We work closely with international organisations and fora to shape global privacy standards and tackle cross-border challenges. Our collaboration extends beyond the EU, engaging with organisations like the Global Privacy Assembly, OECD, and G7, in the context of the Data Protection Authorities Roundtable.

By sharing expertise, we help promote a coherent regulatory approach that respects individuals' rights globally. We also support joint initiatives and technical fora to promote data protection, consumer rights, and fair digital markets. This international engagement ensures that emerging technologies are developed and deployed with strong safeguards. Such efforts are crucial for addressing issues like AI ethics, Data Free Flow with Trust (DFFT), and the harmonisation of regulatory practices across borders.



4.9.1.
G7 DPA Roundtable 2024: shaping the future of AI

From 9 to 11 October 2024, we participated to the G7 Data Protection Authorities Roundtable (DPA) in Rome, Italy together with representatives from Canada, France, Germany, Japan, the United Kingdom and United States. The EDPB and the EDPS are together representing the EU at the G7 Roundtable meetings.

This annual event, hosted this this time by the Data Protection Authority of Italy, Garante per la Protezione dei Dati Personali, focused on three core areas: Data Free Flow with Trust (DGGT), the implications of emerging technologies, and enforcement cooperation.

One of the key outcomes of the G7 DPA roundtable was the adoption of a "Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI" highlighting the crucial role of DPAs in ensuring that AI technologies uphold fundamental rights and are used responsibly.

Additionally, the G7 DPAs issued a "Statement on AI and Children" calling for urgent action to safeguard children's privacy. It emphasises the responsibility of all stakeholders to ensure that emerging technologies, such as AI, promote trust while protecting the most vulnerable.

The G7 DPAs also adopted:

- a Comparative analysis of core elements of the EU GDPR certification as a tool for transfers and of the Global Cross-Border Privacy Rules (CBPR) System in a data controller-to-controller scenario;
- a Terminology paper related to the notions of anonymisation, pseudonymisation and de-identification;
- a document on "Promoting Enforcement Cooperation";
- the G7 DPAs Communiqué; and
- the 2024/2025 G7 DPAs Action Plan.

The next meeting of the G7 DPAs roundtable will take place from 17 to 19 June 2025 in Ottawa, Canada.

4.9.2. Global Privacy Assembly

We contributed to the activities of the Global Privacy Assembly (GPA), an international forum that brings together more than 130 data protection and privacy authorities from across the globe. The GPA takes place every year. The 2024 edition was hosted by the Personal Data Protection Authority of Jersey from 28 October to 1 November.

The EDPS, jointly with the data protection authority of France (CNIL), co-chairs the GPA working group on Ethics and Data Protection in AI (AIWG).

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

- global frameworks and standards;
- the digital economy and society;
- data protection and other rights freedoms;
- international enforcement cooperation;
- digital citizen and consumer;
- the role of personal data in International Development Aid, International Humanitarian Aid and crisis management;
- data sharing.

During the closed session, we presented, together with the CNIL, the report of the AI and ethics WG and reported on the activities of the Council of Europe as EDPS is representing the GPA as observer to the T-PD.

The GPA adopted a number of resolutions:

- a Resolution on Data Free Flow with Trust (DFFT) which was sponsored by the EDPS and the Federal Data Protection Commissioner (BfDI) of Germany. The resolution aims to foster the discussion on Data Free flow with Trust and foresees a number of concrete initiatives and follow-up actions;
- a Resolution on neurotechnologies with EDPS as co-sponsor;
- a Resolution on certification;
- a Resolution on the rules of procedure establishing a hybrid voting on closed sessions as proposed by EDPS.

4.9.3. European Conference of Data Protection Authorities

With the other DPAs s of EU Member States and the Council of Europe, we met for the 32nd edition of the European Conference of Data Protection Authorities (the "Spring Conference") on 14-16 May in Riga, Latvia. The Spring Conference addresses data protection issues, emerging trends and new developments relating to the rights to privacy and data protection. This fora also serves as a way to promote cooperation between the different European countries and exchange best practices.

The European DPAs adopted a Resolution on enhanced cooperation. The resolution reflects the commitment of European DPAs to collaborate closely in addressing the challenges and possible opportunities presented by the borderless nature of data processing, thereby upholding the fundamental rights and freedoms of individuals in the digital age.

4.9.4. Council of Europe

The EDPS participates as an observer in the Consultative Committee of the Convention 108 (T-PD) which is responsible for interpreting provisions of the Convention 108 so that they can be applied practically as the first legally binding international instrument in the data protection field. In this capacity, we actively contribute to the discussions and provide comments on the documents prepared by the T-PD.

Convention 108 has been modernised to address challenges resulting from the use of new information and communication technologies and to strengthen the Convention's effective implementation.

Once it has obtained 38 ratifications, the Protocol modernising the Convention will enter into force. In March 2025, 5 ratifications were still missing for such entry into force. We continue to support the efforts of the Council of Europe to promote the ratification of the Protocol.

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

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

- facial recognition;
- artificial intelligence;
- oversight of intelligence services;
- digital identity;
- processing of personal data in the context of political activities and elections;
- contractual clauses in the context of trans-border data flows;
- inter-state exchanges of data for Anti-Money Laundering/Countering Financing of Terrorism, and tax purposes;
- privacy and data protection implication of the use of neurotechnology and neural data from the perspective of Convention 108+;
- the use of Privacy enhancing technologies (PET) with regard to the processing of synthetic data and large language models.

The T-PD Committee developed the Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law, which is the first-ever international legally binding treaty in this field. The goal is to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law, while being conducive to technological progress and innovation.

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

The CAI has now developed a methodology called HUDERIA to guide and assist with identifying contexts and applications where the deployment of AI systems could pose risks to human rights, the functioning of democracy and the observance of the rule of law, and to assess and mitigate these risks.

The new EDPS office in Strasbourg also provides an opportunity for closer cooperation and engagement with policymakers with the objective to reinforce the cooperation with other European institutions present in Strasbourg such as the European Court of Human Rights and the Council of Europe.

4.9.5. Organisations for Economic Co-operation and Development

The OECD's work that is relevant to data protection primarily carried out by the Working Party on Data Governance and Privacy in the Digital Economy (DGP), the activities of which we actively follow.

The EDPS participates in the Privacy Guidelines Expert Group (PGEG), as well as in the expert community to support the process of building trust surrounding data and its use across borders, set up to support the DFFT initiative.

This community gathers experts from governments, academia, civil society, business, and international organisations to provide project-based technical perspectives and evidence to the policy-oriented work of the OECD.

4.9.6. EDPS – Western Balkans and Eastern Partnership Region

Building on the success of the first high-level event on Data Protection in the Western Balkans and Eastern Partnership Region, organised by the SIGMA Programme; the Eastern Partnership Regional Fund for Public Administration; the Regional Cooperation Council and the Regional School of Public Administration last year, the EDPS had the honour of welcoming authorities from Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Kosovo, Moldova, Montenegro, North Macedonia, Serbia, and Ukraine in the context of a Western Balkans and Eastern Partnership Region's Data Protection Academy.

The event provided an opportunity to exchange experiences, challenges, and best practices in upholding individuals' privacy rights. The Academy, held in September, included a full day of discussions at our headquarters, where participants explored the practical application of data protection rules and emerging regulatory challenges.

During these exchanges, Supervisor Wojciech Wiewiórowski underlined the importance of continued international cooperation to uphold high data protection standards in line with shared values. We also presented our strategy on Artificial Intelligence, addressing both opportunities and risks associated with AI development, while ensuring compliance with data protection principles. The discussions covered various topics, including the interplay between the GDPR and new European regulations, enforcement strategies, and cross-border data transfers.

INTERNATIONAL ORGANISATIONS WORKSHOP ON DATA PROTECTION



Since 2005, the International Organisations Workshop on Data Protection (IOW) aims to bring together International Organisations to share experiences and best practices in the field of privacy and data protection. Participants discuss the most recent regulatory developments at international level and analyse their implications for International Organisations.

WHY PARTICIPATE?

- Meet other International Organisations
- Discuss recent data protection challenges
- Share experiences and best practices
- Exchange on common issues
- Be part of a Community

WHO CAN PARTICIPATE

The IOW is reserved for members of International Organisations who deal with data protection matters.

ABOUT THE ORGANISERS

Each year the European Data Protection Supervisor (EDPS) organises the IOW with a different International Organisation to reach diverse audiences and explore a wide array of critical topics.

MORE INFORMATION

www.edps.europa.eu

EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

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

4.9.7.
EDPS Annual Workshop with International Organisations

On 23 - 24 September 2024, **we co-organised the 2024 edition of the International Organisations Workshop on data protection (IOW), in partnership with the World Bank, in Washington, D.C.** It was the first time that the workshop was held outside of Europe, reinforcing our commitment to enhancing the global dimension of this initiative and promoting the application of data protection principles worldwide.

Since its creation in 2005, this initiative has served as a platform for discussing pressing issues and promoting high standards in data protection, bringing together International Organisations to share knowledge and best practices for safeguarding personal data.

The EDPS co-organises this workshop each year in a different location and in collaboration with a different International Organisation. The year 2024 was marked by a significant milestone for the EDPS – our institution's 20th anniversary. To commemorate this occasion in the context of the IOW, a high-level panel took a deep dive into the workshop's journey over the past two decades, reflecting on its achievements and challenges while exploring future perspectives for this initiative.

A dedicated panel on AI provided a platform for the participants to explore both the potential of AI and the data protection challenges it brings. The conversation highlighted the importance of sharing best practices to navigate risks associated with the use of AI, ensuring that innovation goes hand-in-hand with safeguarding individuals' privacy.

In addition to these panels, the workshop featured two practical sessions. The first focused on strategies for preventing, mitigating, and responding to personal data breaches, providing participants with actionable insights to enhance their defences. The second session focused on how to ensure that IT tools, whether developed in-house or procured, comply with the highest privacy standards. Finally, the workshop included two breakout sessions to encourage dynamic discussions in smaller groups. One session tackled the complexities of data transfers to and from International Organisations, while the other explored the challenges for DPO's and other privacy professionals within these Organisations. The format of these sessions resulted in a deeper engagement, enabling participants to exchange knowledge and experience in a more personal setting.

CHAPTER FIVE

Technology and Privacy: foresight, oversight and digital transformation



The EDPS **anticipates the evolution of technologies**, and the digital landscape as a whole, their **opportunities for and challenges to data protection** with its dedicated Technology and Privacy Unit.

How? The Unit's activities are three-fold.

The **Technology Monitoring and Foresight Sector** monitors technological developments using a foresight-based approach.

The **Digital Transformation Sector** takes care of the institution's digital innovation by both integrating the European Parliament's IT infrastructure and tools from various European institutions, bodies, offices and agencies (EUIs), as well as procuring open source software to support some of the specific tasks of the EDPS.

The **Systems Oversight and Technology Audits Sector** performs investigations and audits on how EUIs use technology when personal data is processed, in particular for Large Scale IT Systems, mostly relevant in the Area of Freedom, Security and Justice. This sector is also responsible for managing personal data breach notifications communicated by EUIs.

Progress Delivered

In this chapter, we summarise our work of scouting **the opportunities and challenges brought by the digital world**, by:

- **steering technologies' lifecycle** to embed privacy and data protection;
- **supporting EUIs in** preventing, detecting and overcoming **personal data breaches**;
- **providing the EDPS with the right digital environment** and tool to carry out its tasks.

To achieve this we:

- focused our **monitoring and foresight activities on AI**, and other pervasive trends such as neurotechnologies;
- applied our **improved personal data IT security audit practices** and approach for more effectiveness led specific awareness and training actions to strengthen EUIs awareness and preparedness on data breach management such as a personal data breach survey and a cybersecurity exercise;
- streamlined our **IT support** and continued to improve our **auditing IT tools**.

5.1. Technology monitoring and foresight

With the accelerating speed of **digital transformation**, we strive to stay up to date with the latest advancements in information technology.



As part of our work, it is crucial to understand these developments and anticipate technological changes and what they may mean for people's privacy and data protection, so that privacy and data protection principles and features are embedded in the entire lifecycle of technologies, from the early stages of their development.

In this regard, our efforts in 2024 were fuelled by the need to focus on artificial intelligence and its trends.

Our foresight work helps Europe to become more resilient and future-proof, as per our objectives set out in our Strategy 2020-2024.

5.1.1. TechSonar Report 2025

We published our latest TechSonar on AI technologies, presenting six AI trends to watch in 2025. These include:



- **neuro-symbolic Artificial Intelligence** combining neural networks with symbolic **reasoning to enhance accuracy and decision-making processes**;
- **retrieval-augmented generation**, a technique that allows AI systems to generate more relevant output by retrieving and combining relevant information from multiple knowledge bases;
- **on-device AI**: a system architecture designed to place data processing at the edge of the network or not connected at all;
- **scalable oversight** which focuses on the ability to use AI systems to effectively monitor other AI systems;
- **machine unlearning** to enable trained AI systems to forget the use of specific data in training the model;
- **multimodal AI** to simultaneously process information from multiple types of data, from text to images, video or audio.

To help the public understand these complex trends, we used plausible, yet fictional scenarios, demonstrating the potential application of the technology in our daily lives.

5.1.2. TechDispatch and TechDispatch Talks: close up on neurodata



Whilst we attempt to predict emerging technologies and their impact with TechSonar, we also concentrate our expertise in monitoring current technologies, their development and influence on privacy and data protection, with our TechDispatch reports and talks.

Therefore, our TechDispatch Reports and TechDispatch Talks aim to explain, inform and raise awareness of potential data protection issues surrounding technologies.

Each TechDispatch provides factual descriptions of a technology, assesses its possible impact on privacy and personal data protection, and provides links to further recommended reading. With these reports and talks, we aim to foster ongoing dialogue on technologies and data protection challenges whilst promoting data protection by design and by default within innovation processes.

Together with the Agencia Española de Protección de Datos (AEPD), the DPA of Spain, we issued a TechDispatch on neurodata analysing the impact on individuals' privacy and other fundamental rights of using information directly gathered from the brain and/or from the nervous system and the conclusions drawn from on this data, such as emotional cues or preferences.

Whilst this processing can bring progress to clinical medicine and neuroscientific research and allow for progress in treatments for migraine and other disorders. We also dug into the worrying trend of ethically and legally questionable uses of neurotechnologies. An example of this is the use of neurodata for marketing purposes. Some of these practices may be incredibly invasive, pose unacceptable risks to fundamental rights, and be unlawful under EU data protection law.

Read our TechDispatch on neurodata available in English and Spanish.

TechDispatch Talks



Bringing the tech world and its relationship with privacy closer to the public by expanding our reach to a wider audience has also been one of our priorities this year.

In May 2023, we created a podcast series, TechDispatch Talks, available on our website and on Spotify @EDPSOnAir. Mirroring the TechDispatch issues, the podcast's format, a Q&A, allows our in-house experts to examine closely the intricacies of each technology.

With this podcast series, we aim to help both experts and non-experts to understand the aspects of these technologies with concrete examples.



5.1.3.
Pursuing the Internet Privacy Engineering Network (IPEN)

Human Oversight in Automated Decision-Making

In light of the current dynamic AI landscape, we co-hosted with the Swedish University of Karlstad the 10th Internet Privacy Engineering Network (IPEN) event on 3rd September 2024, focusing on human oversight in automated decision-making.

Automated-decision making already influences small or big decisions in our day-to-day lives, from the mundane to the more significant, such as deciding on what to wear, event recruitment processes, and credit scores. We therefore believe it was apt to gather experts in data protection, technologies and other partners to discuss the privacy challenges, opportunities and impact of this phenomenon.

Both the GDPR and the Artificial Intelligence Act address the risks associated with automated decision-making and provide for human oversight as one of the measures to ensure the accountability and fairness of these systems.

With 300 participants attending the event either in person or online, the appetite for exchanges had no limits. Topics touched upon included:

- the way human-oversight can be properly integrated into the use of Artificial Intelligence and automated - decision making to enhance individuals' understanding of how their personal data is processed;
- the possibility of creating standards for automated and non-automated decision-making for a high-level of protection;
- the factors that may influence the effectiveness of human oversight, focusing on technical aspects.

You can find out more about automated-decision making by watching the recorded IPEN event here.

5.1.4.
Cooperating with the EDPB in assessing the impact of technology

Within the EDPS role as member and secretariat provider of the European Data Protection Board (EDPB), we provided our diverse expertise, including our acumen in technology to help inform the EDPB's advisory and supervisory tasks impacting the digital landscape.

This year we gave our advice on the topic of personal data and the anonymisation and pseudonymisation of individuals' personal information, as well as on the use of facial recognition technologies in airports and in the law enforcement context.

We also helped with the organisation of the EDPB mobile app bootcamp, during which experts met to exchange knowledge and best practices and test tools for mobile apps auditing.

Similarly, we supported the EDPB in assessing the impact of AI technologies on privacy and data protection policy, focusing on AI models and data processing, such as "web scraping", a trend to collect any data posted on the public web to train AI models.

5.2. Personal Data Breaches

EDPS awareness campaign on data breaches

In 2024, we launched a campaign to raise awareness of personal data breaches in European Union institutions, agencies, and bodies (EUIs). This initiative was part of a series of actions marking the EDPS' 20th anniversary, and specifically targeting EUIs that had never reported a personal data breach before.

The campaign unfolded in four key phases.

It started with a survey, allowing institutions to assess the maturity of their personal data breach management processes, which we analysed to create a customised personal data breach assessment toolkit. This was followed by bilateral meetings to discuss challenges and areas for improvement. The campaign concluded with a final report, summarising key observations and providing tailored recommendations to strengthen compliance.

One of the most pressing findings was the existence of gaps in staff's awareness and training for the handling personal data. We emphasised that controllers, supported by their institution's data protection officer, should take a proactive role in educating employees on recognising and managing data breaches effectively. Without proper training, many incidents go unnoticed or are mismanaged, increasing risks for both individuals and institutions.

Another critical issue was insufficient resource allocation for personal data breach management. Many EUIs lacked dedicated personnel and financial support to handle personal data incidents. We urged EUIs to invest more to support compliance and personal data breach management.

Finally, the campaign revealed gaps in risk management practices. Many EUIs did not have a structured framework for assessing and mitigating risks related to personal data breaches. We recommended establishing a formal risk management framework to identify and mitigate personal data breaches.

Personal data breaches and cybersecurity incidents

Together with the European Union Agency for Cybersecurity (ENISA), a regular partner of ours, we hosted the very first **Personal dATa bReach awareness In Cybersecurity Incident hAndling (PATRICIA)**, a hands-on exercise designed to test how well EUIs respond to personal data breaches. Held at the EDPS headquarters in Brussels, the event's goal was to assess how responsibilities are distributed during a breach, increase awareness of risks to individuals, and improve collaboration between cybersecurity and data protection teams.

The exercise brought together 21 participants from six EUIs, including IT managers, Data Protection Officers (DPOs) and Local Cybersecurity Officers (LISOs). CERT-EU, the Computer Emergency Response Team for EU institutions that took part as an observer, offering insight into incident response strategies. The event was split into two sessions. The first simulated real-world cybersecurity incidents, challenging teams to react using their internal processes, assess risks, and coordinate their response. The second session was a debriefing, where participants reflected on their decisions, examined the effectiveness of their responses, and identified areas for improvement.

Key challenges emerged during the exercise. To address them, the EDPS and ENISA recommended increasing senior management involvement to create a more structured response framework, clearly defining stakeholder responsibilities to streamline decision-making, strengthening training programs, and encouraging closer cooperation between cybersecurity and data protection professionals.

Going forward, we are planning to renew this experience and involve other EUIs in this exercise.

The exercise underscored the importance of cross-disciplinary teamwork and showed how cybersecurity and data protection authorities like the EDPS can work together to build resilience and improve personal data breach response across EU institutions while protecting people and their personal data.

Legal obligations with personal data breaches

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

Under Regulation (EU) 2018/1725, all EUIs have a duty to report personal data breaches to us, unless a risk to the affected individuals is unlikely.

All EUIs must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to pose a high risk of adversely affecting individuals' rights and freedoms, the EUI must also inform the concerned individuals without unnecessary delay. These obligations apply also for breaches on 'operational personal data'.

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

Administration of incoming personal data breach notifications

2024 marks a year where the number of data breaches notified to the EDPS grew in number and also in complexity. Still, the EDPS successfully managed to provide a much quicker response than in previous years and reduced the backlog of cases substantially.

All cases up to 2022 are now closed and most of the cases received in 2023 and 2024 are either closed or show good progress. Concerning the cases of 2023, more than 90% are handled and closed. With regard to the 2024 cases, the number of cases closed reaches 50%.

Driving progress in handling personal data breaches

In 2024, we undertook several initiatives to strengthen compliance with personal data breach management, reinforcing our supervisory role under Regulation (EU) 2018/1725, which obliges EUIs to take precautionary measures and effective procedures to prevent personal data breaches as these can cause serious harm to individuals.

In February 2024, a pre-investigation was initiated into the security measures of a widely used institutional tool, assessing its compliance with:

- responsibility of the controller;
- data protection by design;
- responsibility of the processor;
- security of processing;
- confidentiality of electronic communications.

This pre-investigation helped verify whether EUI's existing technical and organisational safeguards were sufficient to mitigate risks and prevent data breaches.

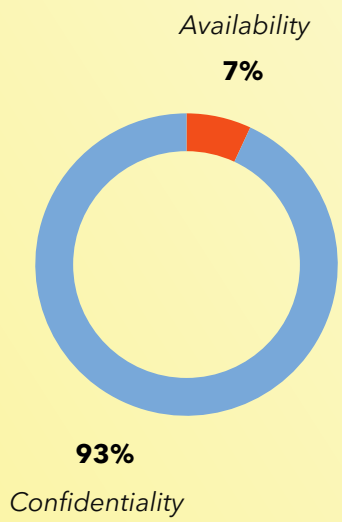
Additionally, in response to a large-scale cyberattack affecting an EUI, we issued a Supervisory Order instructing them to notify affected individuals within a specific deadline. We have the power to issue these types of orders under Regulation (EU) 2018/1725 to ensure EUIs comply with their legal obligations to inform individuals whose personal data have suffered a breach involving a high risk for them, put in place corrective measures, and strengthen data security practices.

5.2.1.
By the numbers: personal data breaches in 2024

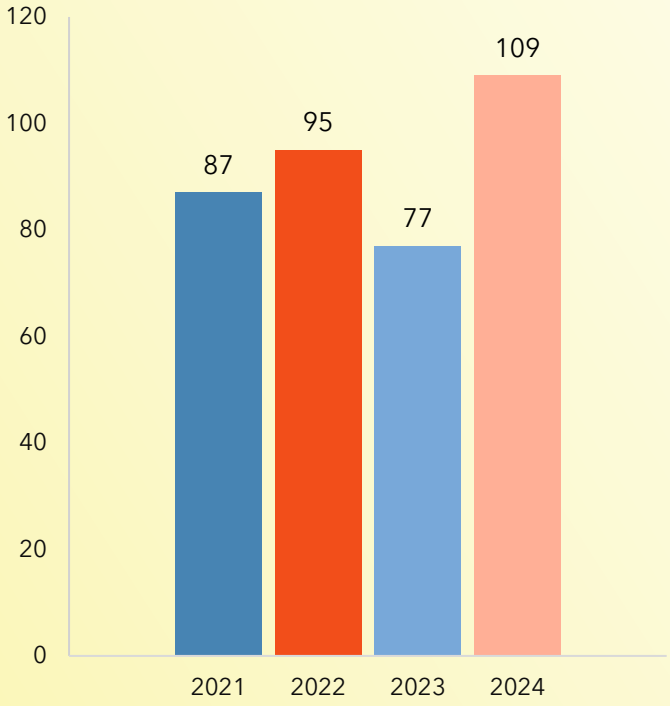
In 2024, we received and assessed 109 new admissible personal data breach notifications under Regulation (EU) 2018/1725.

Overall, there was nearly a 30% increase compared to 2023, during which we received 77 personal data breaches.

Out of 109 submitted data breach notifications, 101 cases pose data breach of confidentiality whereas 8 cases posed mainly availability breaches. Only one case included a breach of integrity.



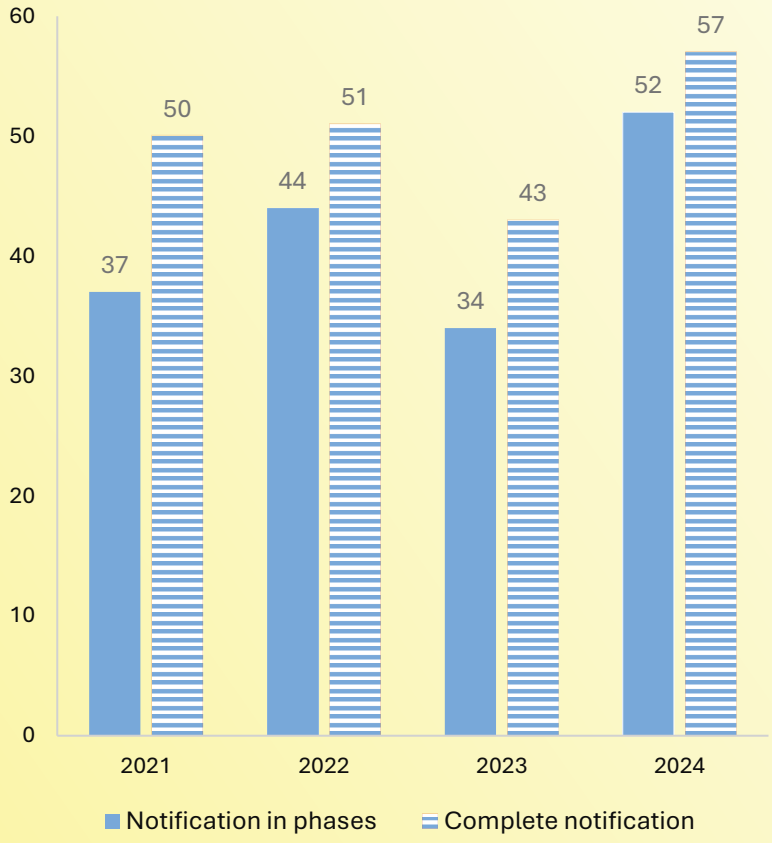
Primary types of personal data breaches in 2024



Number of Personal Data Breach Notifications for the years 2021-2024

In 2024, we received 57 complete personal data breach notifications and 52 notifications in phases. By the end of 2024, not all notifications in phases had been yet finalised from the relevant EUIs.

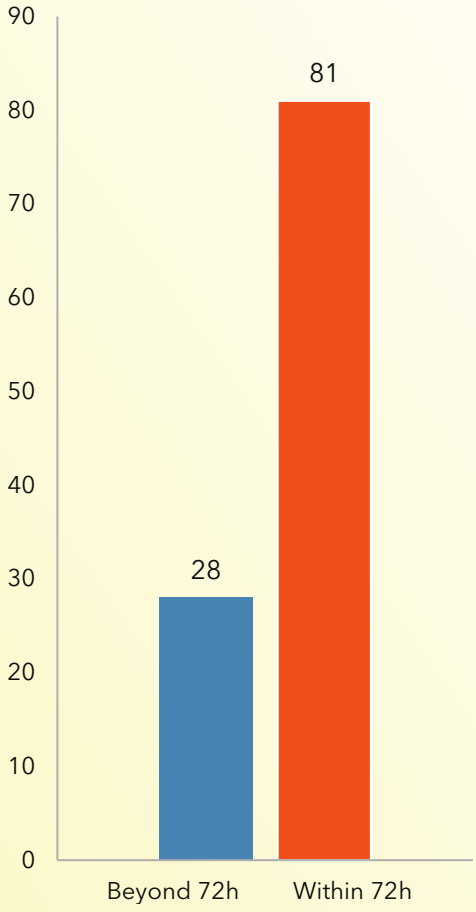
As shown below, during the last 4 years (2021-2024), the proportion of comprehensive notifications and notifications in phases did not differ significantly in comparison to the previous years.



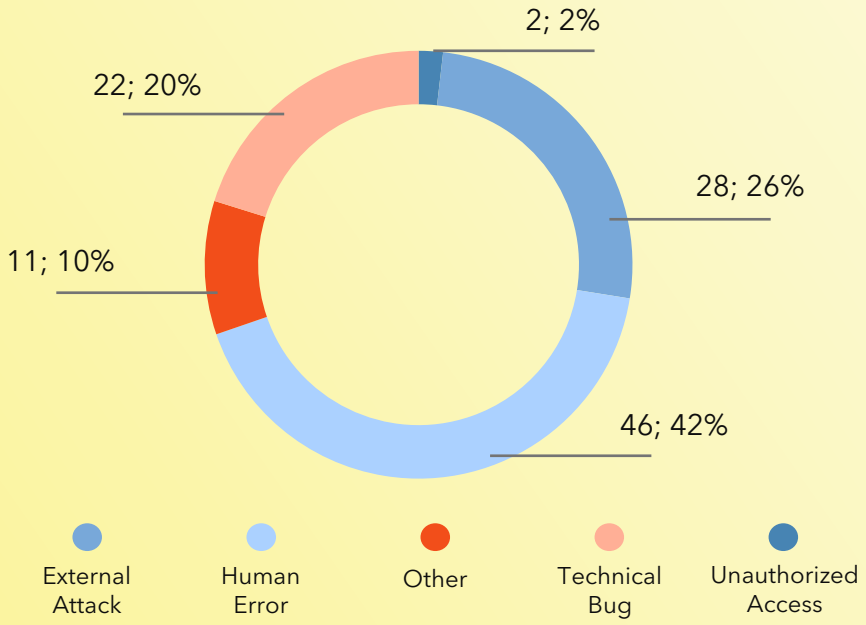
Type of Data Breaches Notification
Category Complete vs In Phases

Concerning the notification of personal data breaches within 72 hours, 81 notifications were submitted within 72 hours, whilst 28 notifications were delayed by the controllers due to various reasons. In some cases, the delay was justified, as for example for cases with ongoing investigations trying to identify how individuals' personal data were affected. In some other cases, delays occurred due to lengthy internal procedures of the controllers concerning the final approval of the notification. In the latter, we advise the EUIs to review and simplify their internal processes for personal data breach notifications in order to meet the legal deadline and thus meet the accountability principle.

In comparison to last year, we could interpret the identified 2024 figures as a major improvement for all reporting institutions in managing internally the occurred data breaches as the number of cases be-yond the 72 hours significantly decreased.



Number of data breaches Notification within 72hours in 2024



Root Cause of Personal Data Breach Notifications in 2024

This year, **human error** remains the most common cause of personal data breaches.

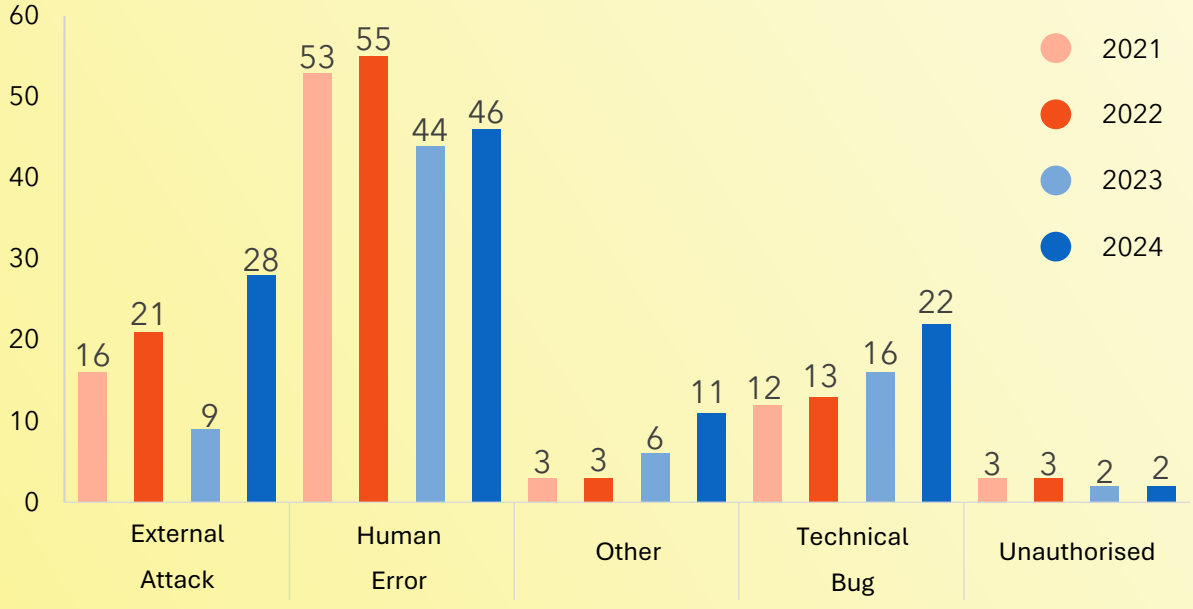
In these cases, the usual pattern observed is that a person/EUI staff sends an email with confidential information to the wrong recipients or puts all recipients in carbon copy (cc) instead of blind carbon copy (bcc), whereas their contact details should not to be disclosed to the rest of the recipients list.

Similarly, some personal data breach notifications concern documents published without removing personal data, in the context of EUIs' access requests and transparency procedures.

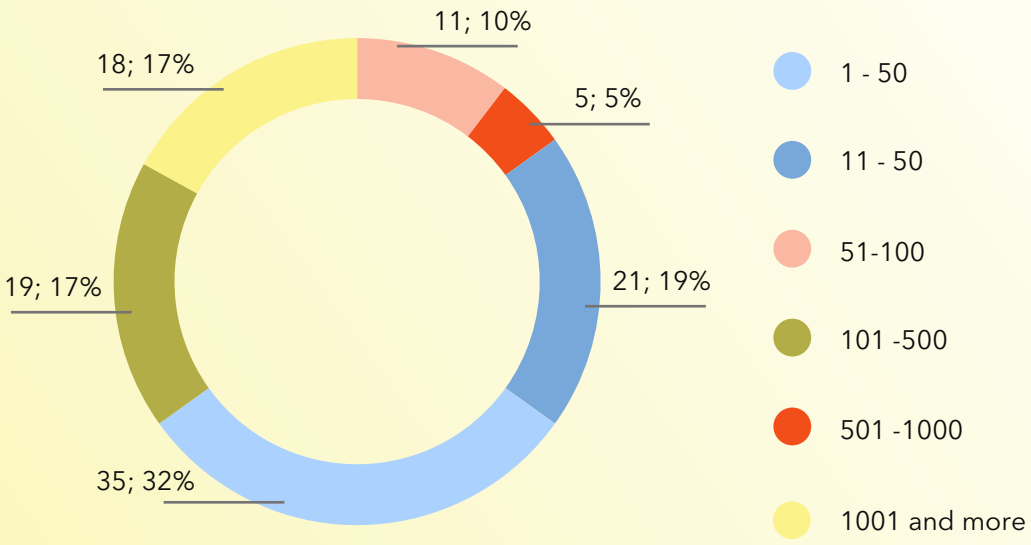
Like in previous years, a high number of human errors occur during recruitment processes. For example, results of selection processes were sent to the wrong candidates. Other breaches involving human error include the sending of medical or financial information to the wrong recipients.

Contrary to 2023, personal data breaches caused by external attacks comes in second place of the data breaches we received. There was an increase of just above 2% between 2023 and 2024. In many cases, these attacks are due to insufficient security measures and procedures in EUIs, such as secure design, secure coding and patching of systems. Examining these type of breaches, we noted the absence of data protection by design and effective measures, which could have helped avoid the incident, such as setting and managing data retention periods to minimise the impact of the attack.

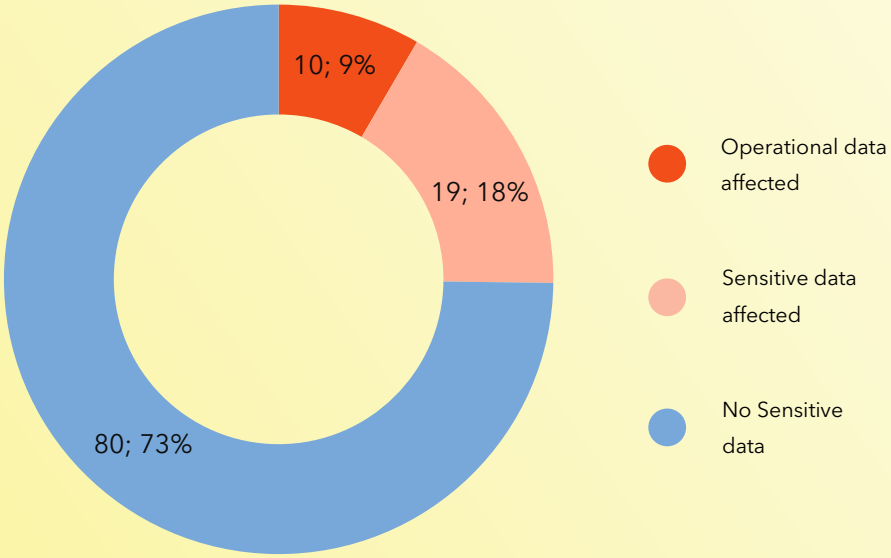
Behind external attack causes comes personal data breaches caused by a technical bug, increasing by 4% since 2023. These bugs may be linked to misconfiguration of access rights or other mal-configured features, due to a lack of testing or review of the tool pre and post



Root Cause of Personal Data Breach Notifications : from 2021-2024



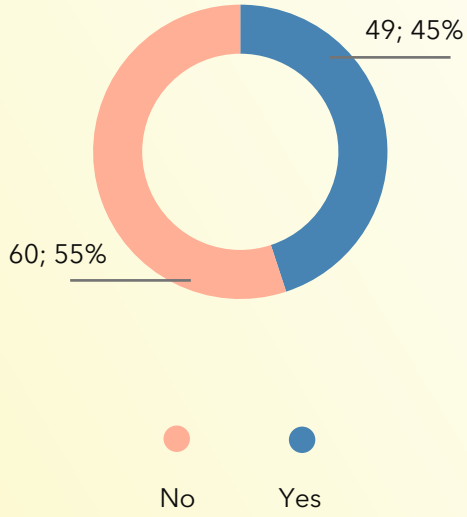
Number of affected individuals per data breach notification in 2024



Categories of personal data in data breach notifications in 2024

18% of personal data breach notifications received this year concerned special categories of data, especially health data, due to errors when sending medical invoices in the case of the reimbursement processes. In these circumstances, we recommend that EUIs raise their staff's (or contractors') awareness on the matter, and consider additional safeguards to avoid human error.

In 9% of the personal data breach cases, the confidentiality of operational personal data was impacted. The categories of persons affected included suspects and individuals under investigations, as well as information related to officers being assigned specific tasks. Regarding the personal operational data breach notifications we received, no special categories of data were concerned.



Notification to the data subjects in 2024

Communication to individuals in 2024

In 49 cases, EUIs decided to communicate the personal data breach to the individuals concerned. Whilst some were obliged to do so, due to the high risks for individuals, others decided to notify the individuals as a matter of transparency. We acknowledge this effort and may even propose this option to EUIs when there is a sensitive context to the data breach.

In 2024, one data breach that posed such high risks to individuals it triggered us to issue a supervisory order for the EUI to communicate to these individuals in compliance with the law. Since sometimes we are notified of personal data breaches in phases, in these cases further analysis and assessments of the risks may evolve.

Inadmissible data breach notifications

We also received four notifications that did not need notifying to the EDPS. In these cases, we assessed there was an unlikely risk posed to individuals and we therefore informed EUIs to document the breach in their internal register.

We also received 12 notifications sent from private companies or individuals (whistle-blowers), which were outside the scope of the EDPS' legal competence. These were either from companies having a main establishment in the EU, in which case the corresponding EU national data protection authority under GDPR would be competent. Other notifications falling under this category were from companies processing data of EU citizens, without an establishment in the EU.

5.3.
Overseeing IT systems and auditing tech

Visa Information System: strengthening security

Auditing the EDPS Visa Information System (VIS) is a legal obligation that we carry out every four years to assess the processing of personal data by eu-LISA, the EU agency responsible for managing large-scale IT systems in the area of freedom, security, and justice. The audit follows international standards, notably ISO 27001 and ISO 27002, which outline best practices for information security management.

In 2024, we focused on specific security and data protection aspects of VIS, identifying several functional and security-related concerns. These findings warrant further attention from eu-LISA's management, and we will issue recommendations to address them.

The final audit report is expected in 2025.

Schengen Information System: advancing data security

As part of its supervisory role, we conducted an audit follow-up to assess if and how our recommendations issued in our previous audit report on the Schengen Information System (SIS), the Visa Information System (VIS), and the European Asylum Dactyloscopy Database (EURODAC) were put in place. We found that 21 recommendations were put in place, marking significant progress in strengthening security and data protection measures across these systems. To ensure full compliance, we will follow up on our audit in 2025, reviewing the remaining recommendations from the 2023 report.

5.3.1.
Updates on audits of EU institutions' websites

In August 2024, we completed the second and final phase of our remote audits of EUIs' websites, delivering 17 compliance reports to 13 EU institutions.

EUIs rely on their websites to provide services and information, with maps, videos, and interactive tools, sometimes supported by third parties. These features can introduce potential risks to personal data.

We examined how key data protection requirements under Regulation (EU) 2018/1725 are followed, focusing on secure website communication, user tracking technologies, and the transparency of information provided to visitors.

The audits were conducted using our enhanced Website Evidence Collector (WEC) (see section 5.7). Each report includes tailored recommendations to address identified non-compliance issues.

We will follow up on our recommendations in 2025 to ensure adherence to data protection standards.

5.3.2.
Raising awareness to achieve compliance of EUIs websites

We launched the Website Compliance Awareness Campaign (WCAC) to help EUIs improve their websites' compliance with data protection rules. This is an action that we carry out to encourage EUIs to manage their website compliance in an accountable way.

To help in this area, we this aim, we offer the Website Evidence Collector. While WEC has been available since 2018, its awareness and use among EUIs has remained low. The WCAC aims to bridge this gap by systematically scanning websites and generating simplified reports that highlight potential compliance issues.

The campaign follows a structured approach: the first wave of scans took place in autumn 2024, with results presented at the DPO meeting in Luxembourg in November 2024. The initiative was well received with DPOs acknowledging the benefits of proactive monitoring. The second wave is scheduled for 2025, followed by a final wave in autumn 2025. After each round, institutions will receive individual reports and recommendations along with reminders to use the WEC tool for self-assessment.

At the end of the pilot phase, we will assess the possibility of expanding the campaign to cover all EUI websites, which exceed 1,300. While the WCAC is designed to raise awareness and promote voluntary compliance, this does not prevent us from launching formal investigations or audits if necessary.

By fostering transparency and accountability, the initiative aligns with our continuous mission to enhance data protection in the digital administration of the EU.

5.4.
EDPS decentralised social media pilot: the end of a successful story

Two years ago, the EDPS launched two social media platforms, EU Voice and EU Video. The pilot project has proved successful in delivering alternative, privacy-friendly and user-focused social media platforms. It is time to review the results.

The two platforms are part of the free, open-source and decentralised social media networks, based on Mastodon and PeerTube. Over the past two years, EUIs had the opportunity to create accounts on the platforms and connect with users registered in the Fediverse, an online network of platforms and services interconnected with each other, including social media platforms.

Initially due to run for one year, the pilot project of EU Voice and EU Video was extended for a second year, due to its success amongst EUIs and its users. By the end of the pilot project, EU Voice hosted 40 institutional accounts, including EU Commissioners and Members of the European Parliament, and EU Video hosted 6 accounts, making EUIs the largest group of public bodies present on the Fediverse globally.

The EDPS' pilot project of EU Voice and EU Video proves that community-driven and decentralised social media platforms may prioritise users' fundamental rights to privacy and personal data and foster the EU's digital sovereignty. Thus, these platforms are possible tangible and viable alternatives to commonly used social media platforms. While this two-year pilot project presented challenges to secure continued support and dedicated resources, its legacy serves as a testament that collaborative efforts and solutions to shape a safer digital future for the EU are possible.

We will facilitate the required migration of EUIs who wish to keep their accounts active in the Fediverse, by providing the necessary support to ensure a smooth transition to other platforms. EU Voice and EU Video were officially closed on 18 May 2024.

Following the success of this pilot project, we remain committed to exploring innovative solutions that empower both public bodies and citizens in the digital sphere.

5.5. The International Working Group on data protection in technology

The International Working Group on Data Protection in Technology – also known as the Berlin Group – is a global forum that brings together DPAs and privacy experts from around the world to shape a human-centric approach to emerging technologies and provide related guidance. The EDPS has always been an active team player in this international forum. Most recently, we have extensively contributed to the issuance of Working Papers in particular co-leading the one on Central Bank Digital Currency. Leveraging foresight and international collaboration, sharing best practices and lessons learned, the Group works to develop robust guidelines that help manage risks while reaping the benefits of new technological advancements. This collective effort is seen as essential to ensure that technologies evolve in ways that protect individual rights and promote privacy-enhanced environments.

The EDPS co-hosted the 74th meeting in Brussels in November 2024. This two-day meeting was an opportunity for members of the Group to share their views, experiences and challenges on the evolution of technologies, such as neurotechnologies and extended reality, and their potentially high impact on people.

During the discussions, the EDPS took the opportunity to present its recently published TechSonar focusing on different AI technologies. This gave the opportunity to realise how the rapid progress in the field of AI, combined with the potential for high returns on investment, is fuelling an AI race that pose significant pervasive risks to individuals if not properly managed. It is our responsibility to collaborate on ensuring that human dignity is prioritised in the development of AI solutions.

5.6.
Digital transformation in action

The EDPS continues its digital transformation, under the leadership of the Technology & Privacy Unit.

In 2024, we integrated EU Send, a communication tool managed by the European Commission, to facilitate the secure exchange of sensitive, non-classified data such as information on health. This tool allows the exchange with parties of big sets of Sensitive Non Classified information. The goal is to use this tool in the context of the CSC (Committee for the Coordinated Supervision of Large Scale IT Systems) to exchange with EDPS and controllers.



We also streamlined the IT support through Service Now. This upgrade means that, starting early 2025, our staff will benefit from a single IT helpdesk portal regardless of whether the service is provided by the European Parliament or the EDPS.

Additionally, we collaborated with the European Commission and Parliament to adopt SECABC, a solution that enables encrypted email communication across all participating EUIs.

5.7.
Website Evidence Collector updates

The Website Evidence Collector (WEC) is a vital EDPS tool designed to capture and analyse digital evidence from websites. Its primary purpose is to monitor how websites implement data protection measures, including the use of cookies and tracking technologies. The tool allows inspectors to systematically gather evidence, assess compliance with data protection standards, and ultimately ensure transparency in online data practices.

In 2024, we focused on enhancing the WEC by releasing several new minor versions. These updates have improved the tool's stability and performance, providing a more user-friendly interface and faster data processing. Key improvements include enhanced data visualisation capabilities, streamlined evidence export functions, and refined analytical features that help inspectors quickly pinpoint potential privacy issues on websites.

Additionally, the updates have improved integration with other of our inspection software, enabling a more cohesive workflow during audits.

These incremental enhancements are part of a strategic roadmap leading to a major release scheduled for 2025. This future release will further elevate the tool's functionality and adaptability, ensuring that the EDPS can continue to lead in digital privacy oversight.

5.8. Nextcloud

Nextcloud is an open-source cloud solution that enables secure file sharing, messaging, video calls, and collaborative document drafting.

In February 2023, we began piloting Nextcloud together with Collabora Online, a LibreOffice-based tool providing a secure, unified platform for EUIs to work together while keeping personal data within the EU. By negotiating a contract with an EU-based service provider, we ensured that data is processed under strict EU data protection rules, avoiding transfers to non-EU countries and eliminating reliance on monopoly providers. This approach supports the digital strategy of the EU and offers a cost-effective alternative to conventional cloud services.

In 2024, the project focused on migrating Nextcloud's deployment from the initial setup in a private service provider to the European Commission's own data centre, for enhanced control.

This migration leverages existing infrastructure and strengthens data sovereignty, while providing a template solution that can be adopted by other institutions under similar conditions.

5.9. Cyber Europe 2024

The EDPS participated as an observer in Cyber Europe 2024, a large-scale cybersecurity exercise organised by the European Union Agency for Cybersecurity (ENISA). Held every two years since 2010, the 2024 edition focused on the resilience of the EU energy sector. By simulating real-world cyber crises, the exercise tested participants' ability to respond to complex and evolving threats that could disrupt critical energy systems.

Cyber Europe 2024 gathered over 1,000 participants from 30 countries, including 27 EU Member States, Switzerland, Norway, and the UK. Stakeholders from the energy sector, EU institutions, cybersecurity agencies, and international organisations took part. The scenario covered multiple sectors, including electricity, gas, digital infrastructure, media, and public administrations. Participants faced challenges such as Distributed Denial of Service (DDoS) attacks, supply chain disruptions, cyberattacks on industrial systems, and extreme weather events.

An important part of the exercise was a simulated data breach. While the breach did not directly involve EUIs, it provided generally valuable insights into how organisations detect, contain, and mitigate cyber incidents. By observing these responses, we gained a deeper understanding of cybersecurity challenges affecting critical infrastructure and the protection of personal data.

5.10.
Cybersecurity Regulation: an evolving role for EDPS

The new Cybersecurity Regulation 2023/2841 has introduced significant changes for the EDPS and its Technology & Privacy Unit.

This Regulation aims to establish a high common level of cybersecurity across EUIs and reduce risks in digital environments.

Under the Regulation, we now serve as a permanent member of the Inter-Institutional Cybersecurity Board, tasked with monitoring cybersecurity measures and responding to urgent action calls. Union entities must now develop internal cybersecurity frameworks, conduct regular maturity assessments, and allocate a fair share of their ICT budgets to security.



The impact is twofold. First, as a board member, we actively participate in strategic discussions and compliance activities. Second, the Regulation identifies the EDPS as an organisation subject to the Regulation and compels us to enhance our risk management practices. The involvement of the EDPS Technology & Privacy Unit is beneficial to improve its contribution to the EDPS, in particular through initiatives in coordination with CERT-EU, promoting joint activities, and improving training programs and data breach exercises.

CHAPTER SIX

Artificial Intelligence: preparing for the EDPS' future



Since the entry into force of the AI Act on 1 August 2024, the EDPS is now the competent market surveillance authority for the supervision of AI systems developed or deployed by European institutions, bodies and agencies.

The AI Act also designates the EDPS as notified body for conformity assessments of certain high-risk AI systems. Furthermore, the EDPS is competent to investigate complaints by individuals against such AI systems or also to fine the EUIs if they do not comply with the AI Act. The EDPS dedicated much time and effort to prepare its strategy for the use, development and deployment of AI by the EUIs and initiated organisational and procedural preparations for an effective enforcement of the AI Act in the future.

Progress Delivered

This chapter is about how **the EDPS is preparing for its evolving role under the AI Act**.

We have:

- **created the AI Unit**;
- **developed a strategy** centred on governance, risk management and supervision;
- set up the **AI Correspondents network**.

6.1.
Creation of the AI Unit

Recognising the transformative impact of artificial intelligence, we established its AI Unit. This decision reflects our commitment to ensuring that AI systems used by EUIs comply with the Artificial Intelligence Act, at the same time that they uphold fundamental rights, privacy, and data protection principles.



The AI Unit was created on 1 October 2024, to address new supervisory tasks assigned to the EDPS by the AI Act.

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 EUIs 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, we 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.

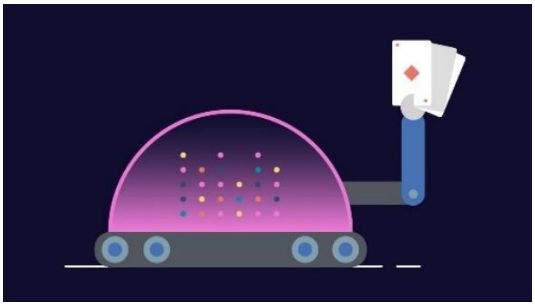
Since its launch, the AI Unit has actively participated in the AI Board and its subgroups, shaping the implementation of the AI Act alongside Member States. It collaborates with the European Commission's AI Office and other EU bodies to ensure consistent AI oversight.

To strengthen our expertise, we invested in specialist recruitment and training, including AI risk management courses and international cooperation with the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe.

Through 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 EU institutions. We are therefore intensively prepared for our new roles and powers under the AI Act.

6.2.
Our plan for Artificial Intelligence in the EU Institutions

The EU Artificial Intelligence Act entered into force on 1 August 2024. This new Regulation brings both opportunities and challenges for EUIs. AI can improve efficiency, support scientific research, and enhance decision-making. However, if misused, it can also pose risks, especially to fundamental rights and privacy.



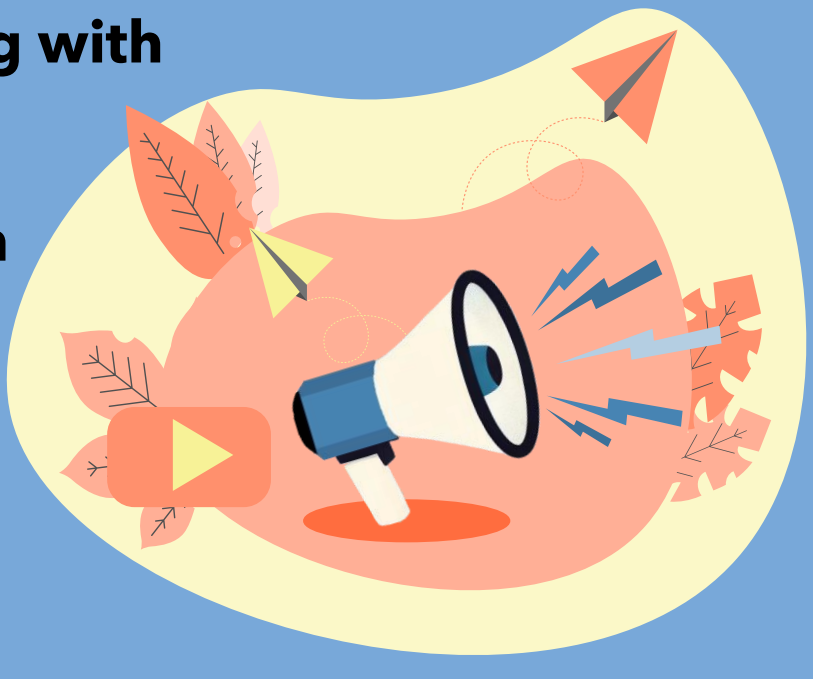
As the AI systems Supervisor for EUIs, we have a clear role: ensuring that AI is used responsibly. To achieve this, we have developed a structured plan based on three key areas.

- **Governance**: Institutions must have clear rules on how AI systems are used. We are working to establish guidelines, policies, and best practices to ensure compliance with the AI Act. Moreover, we have created a solid network of AI Act Correspondents to ensure an adequate and coordinated AI governance across EUIs.
- **Risk Management**: AI systems must be assessed for potential risks to privacy and fundamental rights, so we are developing tools to evaluate and mitigate AI-related risks in EU institutions. Risk Management balances AI innovation with safety measures, urging institutions to allocate resources for AI risk mitigation, like cybersecurity investments.
- **Supervision**: We will monitor and enforce compliance with the AI Act. This includes audits, investigations, and oversight mechanisms to ensure AI tools meet ethical and legal standards. Supervision focuses on prohibiting high-risk AI applications, such as biometric categorisation, emotion inference, and facial recognition, ensuring fundamental rights are upheld.

By putting in motion this plan, we aim to create a safe and transparent AI governance framework within EUIs, balancing innovation with the protection of fundamental rights.

CHAPTER SEVEN

Communicating with impact on data protection



As an organisation, **the European Data Protection Supervisor (EDPS) strives to be transparent - explaining in clear language, accessible to all, what we are doing and why.**

To this end, over the years, the Information and Communication Unit has developed, and cemented, a strong online presence, primarily through our social media channels, and our website. We use these different communication tools depending on the audience we wish to reach, and the type of information we wish to provide. This allows us to both inform the public appropriately on data protection matters and enhance the visibility of our work.

Progress Delivered

This chapter focuses on how we:

- **communicated on the EDPS' 20th anniversary**;
- **diversified our online presence** using different tools, mediums and campaigns;
- **lead events to increase the visibility of our work** to raise global data protection standards;
- **built and maintained relationships with journalists, stakeholders and the public**.

7.1.
EDPS' online presence

With the aim of diversifying our online presence, we have built, and continue to expand, a strong online presence, on our social media channels: X, LinkedIn, Instagram by organising regular social media campaigns, for example. Likewise, we continue to communicate on the EDPS' priorities on our main platform, the EDPS Website.

7.1.1.
Social Media Channels

In this highly digitised world, social media has become one of the most common communication tools. Over the years, we have built a well-established presence on three social media channels, namely X (formerly known as Twitter), LinkedIn and YouTube, and more recently Instagram, which we use to reach a global audience easily and quickly.

Our @EU_EDPS X account allows us to promote the EDPS' presence at a variety of events and to feature the core messages and purpose of our work.



We use our LinkedIn account to communicate with a more specialised audience and other actors interested in the field of privacy and data protection. LinkedIn remains our fastest-growing channel with the highest number of actively engaged followers.

Our YouTube channel serves to post footage from various events, publish awareness-raising videos and broadcast some of the Supervisor's most important speeches. In particular, this year, we used this platform to promote the EDPS traineeship programme with a short, humoristic video.

On Instagram, account opened in February 2024, we share entertaining, educational, fun and playful content, in the form of short videos, carrousels, colourful images and reels on data protection to engage with a different type of audience, mostly young people with a novice level of data protection, and to show how privacy and the digital landscape connects to daily life.

7.1.2.
Social Media campaigns

Using our various social media channels, we planned and executed a variety of social media campaigns, to increase our outreach and keep our audience informed about our activities. Some of our social media campaigns were targeted towards promoting particular initiatives, such as our upcoming events, others allowed us to push past initiatives that our audience may have missed, whilst some campaigns were carried out in partnership with other EU institutions, bodies, offices, agencies. Other times, we used our diverse social media platforms as part of wider communication campaigns.

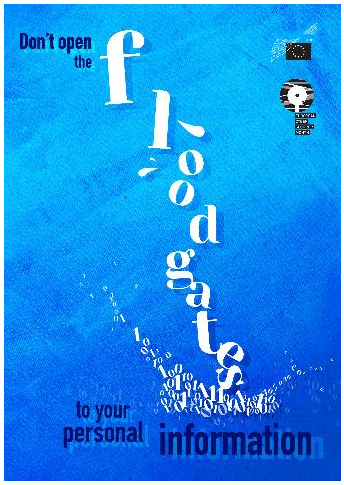
In case you missed it

As we continue to welcome new followers to our ever-growing social media community, we run the #InCaseYouMissedIt campaign on our social media accounts to raise awareness of less high-profile topics and to remind our audience about activities that they might have missed over the past year.



Bluebook Campaign





As part of our commitment to fostering the next generation of data protection professionals, we launched a communication campaign to showcase the experiences of past and present trainees. This initiative aimed to promote the Blue Book Traineeship programme, offering insight into the opportunities and professional growth it provides.

We routinely do this type of promotion by using different formats and mediums, such as videos, testimonials, blogposts, and events.

EU Cybersecurity Campaign

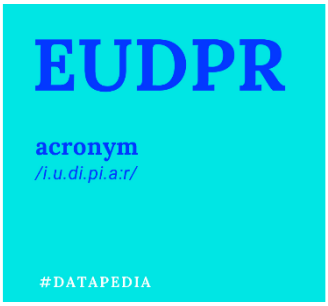
In response to the evolving landscape of cyber threats, we launched a cybersecurity campaign focusing on two critical aspects: cyberattacks leading to personal data breaches and the dual role of AI as both a cybersecurity tool and a potential threat.

To raise awareness, we developed two factsheets exploring these topics in depth. The first addresses the risks associated with cybersecurity breaches, highlighting how malicious actors exploit vulnerabilities to gain unauthorised access to sensitive data.

The second examines the growing impact of AI in cybersecurity, showcasing its potential to automate threat detection and incident response, while also underlining the dangers of AI-powered attacks, such as automated phishing, malware generation, and data exploitation.

Complementing these factsheets, we produced a podcast featuring data protection and cybersecurity experts. The discussion provided valuable insights into how AI is transforming the cybersecurity landscape, emphasising the need for human oversight to mitigate risks. By engaging with a broader audience through these initiatives, we continue to advocate for responsible AI deployment and stronger cyber resilience across EU institutions.

Datapedia: data protection concepts made simple



To strengthen public awareness of privacy and data protection, we launched Datapedia, designed to introduce or reintroduce key concepts in an engaging and accessible manner. This initiative serves as a tool to promote the EDPS' mission, ensuring that individuals and organisations gain a better understanding of data protection.

The campaign features a selection of privacy-related terms from the EDPS Glossary, each presented in a visually appealing format with a clear and concise definition, interpreting and modernising the page of a dictionary with bright colours. By simplifying complex terminology, the campaign enhances understanding of data protection concepts among both specialists and the wider public.

To maximise outreach, Datapedia is deployed across almost all our social media platforms, including LinkedIn, X and Instagram.

With weekly posts every Sunday, the campaign ensures a consistent and structured approach to raising awareness, reinforcing key messages on privacy and data protection in an accessible and informative way.

7.1.3. EDPS Website

The EDPS website is our main communication channel. It is where we host our latest news, press releases, newsletters, podcasts, videos for example; as well as our legal publications, such as our Opinions, Formal Comments, to name a few. One of our priorities is to make sure that our website is user-friendly; therefore, we are continuously improving its features and design, in response to our visitors' feedback and needs. To achieve this priority, we have carried out some more technical actions.

7.2.
Bringing our work one step closer

Data protection continues to be a topic that people, even those who are not experts in the field, care and are interested about, especially since it plays an important part in the evolving digital landscape, with the growing mainstream use of AI. To match this interest, we have diversified our communication products: enhancing our newsletter; further developing our podcast channel; and populating our blog featuring exclusive content from the Supervisor and Secretary General's international activities in data protection.

7.2.1.
EDPS Newsletter

The EDPS Newsletter continues to grow in popularity as an accessible and user-friendly communication tool, suitable for both mobile and desktop users. Now counting 6261 subscribers, the newsletter proves to be an essential communication tool allowing us to respond to our audience's differing interests and levels of expertise concerning data protection matters.

In 2024, we published 8 newsletters to keep our audience up to date with EDPS activities in an approachable, condensed and informative way. Each issue of the EDPS newsletter covered between 7 to 15 topics, ranging from the EDPS' technology monitoring activities, our latest Opinions and Formal Comments, the EDPS' Supervision and Enforcement actions, the EDPS' work as a member of the EDPB, events that the EDPS organised or participated in, to name a few examples.

7.2.2.
Podcasts: monthly updates, bonus episodes and sit down chats

We further developed our podcast series, initially launched in December 2022, with the aim of bringing our audience closer to the work we do to shape a safer digital future, in just under 10 minutes.

Each episode includes a selection of updates on our latest work in the fields of Supervision & Enforcement, Policy & Consultation, Technology & Privacy.

On occasion, we also aired bonus episodes including interviews with selected guests.

To mark the entry into force of the AI Act, we invited EDPS Secretary General Leonardo Cervera Navas to give a more in-depth insight into AI, its opportunities and impact on individuals, society, specific fields, and also to explain the EDPS' new role and responsibilities under this new piece of legislation.



For EU Cybersecurity Month, we hosted a special podcast episode with one of ENISA's cyber experts and one of our very own tech experts to discuss the duality of AI in cybersecurity, as well as data breaches.



This podcast series complements the EDPS' monthly newsletter by sharing our latest activities on a different platform; we aim to cater for our different audience groups.

Whilst establishing this series, we also created another podcast series, TechDispatch Talks, in collaboration with the EDPS' Technology and Privacy Unit, which focuses on upcoming technologies.

All podcasts produced by the EDPS are accessible on our EDPS On Air channel on our website. It is also possible to subscribe to our podcast series via our Podcast RSS Feed. In 2023, we also opened a space on Spotify to increase the accessibility of our podcast content and grow our audience on a specialised platform. There, we strive to create a variety of informative and entertaining content to suit all interests in data protection.

7.2.3.
EDPS blog: a more personal outlook on data protection

The EDPS blog, now active for 8 years, is a platform through which the Supervisor, Wojciech Wiewiórowski, the Secretary-General and, on specific occasions, the EDPS' Heads of Units, are able to communicate on a more personal level about their thoughts, opinions and activities, as well as the EDPS' work in general.

The blog can be easily found on the homepage of our main website where a short extract from the most recent blogpost is always displayed. In 2024, we published 8 blogposts on an array of subject matters.

This year, the blog has served the purpose of narrating the international purpose of data protection, our participation in global fora with the aim of making EU privacy standards a worldwide reality as well as other topics.

7.3.
Public Relations

We frequently interact with the media through press releases, interviews and press events.

7.3.1.
Press releases

This year we issued 12 press releases covering several different areas related to data protection, digital privacy, enforcement and new technological developments. Press Releases aim to inform journalists and other key stakeholders about significant data protection developments and activities that the EDPS has contributed to, such as Opinions on proposed Regulations, enforcement actions, and reports.

Topics covered this year, include updates on our investigations into the EU institutions' use of Microsoft 365, our work in AI preparedness, our leading Opinions and work with other data protection and privacy authorities.



7.3.2.
Public Requests

In 2024, we recorded an increase in public requests for information, submitted by individuals who are keen to learn more about our work, our powers and their rights, when it comes to their personal data. Requests are mainly addressed to us in English, German or French; we always reply in the language in which the request has been written, so long as the request is formulated in one of the EU's official languages. Handling the requests in such manner allows us to convey information promptly to EU citizens or other nationals, externalising our work to various stakeholders and aligning with our principle of transparency. In case of specific requests for which we are not directly competent, we usually refer the requester to the right authority or organisation, inside or outside the European Union.

7.3.3.
Events

The EDPS actively contributed to the organisation, logistical management, and promotion of key events throughout the year, collaborating with co-organisers and, in some cases, shaping the visual identity of the initiatives. These events provided platforms for discussion, knowledge exchange, and policy development in the field of data protection and privacy.

Key Events in 2024:

- **CPDP - Data Protection Day**: A discussion on global privacy challenges and emerging trends, featuring key experts in the field co-organised with the Council of Europe and CPDP Conferences.



- **Press Conference - EDPS Annual Report 2023**: The EDPS presented its annual achievements and future priorities, reinforcing transparency in its work.
- **EU Open Day 2024**: An opportunity to engage with the public and raise awareness on data protection rights, EDPS and EDPB initiatives, with a pool of expert that answered questions on how the Supervisor and the Board protect privacy and data.



- **CPDP - Computers, Privacy and Data Protection Conference 2024**: A major forum organised by CPDP Conferences discussing the intersection of privacy, technology, and digital governance. The EDPS organised two panels on AI and Data Protection.
- **"Consent or Pay: How Can the Single Market and Fundamental Rights Work Together?"**: A debate on the challenges of digital markets and user rights in the era of the Consent or Pay models. The event also showcased the role of both EDPS and EDPB.
- **IPEN Event on Human Oversight of Automated Decision-Making**: A discussion on the role of human intervention in AI-driven decision processes co-hosted by the EDPS and the University of Karlstad. The event delved into the challenges of the human oversight of the AI, discussing the role, the skills and the risk related to AI.

- **International Organisations Workshop on Data Protection 2024**: The EDPS and the World Bank co-hosted the 2024 edition of the International Organisation Workshop on data protection- IOW, a global platform launched by the EDPS in 2005 for international organisations to exchange best practices on data protection.



- **Seminar - Towards a Digital Clearinghouse 2.0**: A session exploring collaborative regulatory approaches in the digital age. In this event relevant stakeholders had the possibility to discuss a position paper and the way forward to ensure a coherent approach to regulatory cooperation in Europe's digital sphere.
- **74th Meeting of the International Working Group on Data Protection in Technology (IWGDPT)**: A high-level gathering to discuss technological developments and data protection implications. The EDPS hosted the 74th meeting of the IWGDPT, were the members discussed topics that ranged from Neurotechnology to Immersive Technologies.

We actively participated in:

- **ECSM Kick-off event**: a 3-day event organised by EESC and CoR to start the European Cybersecurity Month campaign. The event addressed the challenges of today's rapidly changing cyber landscape and the efforts EU institutions to improve cybersecurity. The EDPS participated with a booth and in a panel discussion.

7.3.4. The power of study visits: exploring data protection knowledge

In 2024, 5 study visits were carried out, gathering 170 participants. The reduction compared to the 12 visits of 2023 was determined by the preparation of the 20th Anniversary activities, so we had to reduce the number of accepted study visits. However, study visits remains an essential part of our communication strategy, as a way to connect with our stakeholders.

With this initiative, we aim to raise awareness about our work and the importance of protecting the fundamental rights of privacy and data protection to small groups, mainly university students, or members of national and local governments and other interested groups from across the EU, and beyond.

7.4.
Collaborative Communication

7.4.1.
EU Voice and EU Video

We have continued our close cooperation with EUIs on communication tools and activities. Regarding the management of our alternative social media channels, EU Voice and EU Video, we worked with the European Commission to improve and promote its use amongst other EUIs as well, by highlighting the benefits of these platforms.

This included raising awareness and explaining that these platforms do not rely on transfers of personal data to countries outside the EU and the EEA; that there are no advertisements on the platforms; and that there are no profiling techniques used, meaning that individuals have the choice of and control over how their personal data is used.

Unfortunately, despite our efforts to find a new home for EU Voice and EU Video in other EUIs, we have been unable to secure new ownership to maintain the servers and sustain operations at the high standards that EUIs and our users deserve. (see section 5.7).

7.4.2.
Inter-institutional Online Communication Committee: innovative ideas and support on data protection matters.

We also played an active role in the Inter-institutional Online Communication Committee (IOCC), by providing innovative ideas and support on data protection matters that have an impact on EUIs' communication activities. Through the EU Voice and EU Video projects, we extensively cooperated with the IOCC in order to provide editorial guidelines and servers' policies, accompanying EUIs as they set up their channels on these platforms, prior to its closure. Whilst we provided advice, we also benefited from other EUIs' knowledge, which helped us set up and develop, for example, our automated machine eTranslation tool available on our website. In relation to communication activities, we again joined forces with the European Union Agency for Cybersecurity (ENISA) to develop a campaign for the European Cybersecurity Month.



CHAPTER EIGHT

Celebrating the EDPS' 20th Anniversary

In 2024, we celebrated our 20th anniversary, a milestone reflecting two decades of commitment to protecting privacy and shaping the future of data protection in the EU and beyond. This celebration was not just a moment to look back at past achievements, but also an opportunity to reaffirm the EDPS' role in addressing evolving digital challenges.

Established on 17 January 2004, the EDPS has played a crucial role in guiding EU institutions, bodies, offices and agencies (EUIs) through an ever-changing digital landscape, ensuring that privacy remains a fundamental right in an increasingly data-driven world. From our early days of establishing a robust supervisory framework to its more recent contributions in AI governance and cybersecurity, we have continuously adapted to emerging technologies and regulatory challenges.

The 20th anniversary was structured around four key pillar activities: a book and timeline, 20 talks, 20 initiatives, leading up to a Summit. Each designed to highlight the impact of the EDPS and its vision for the future.

The first pillar consists of a book and a timeline analysing key data protection milestones and the EDPS' influence over the past two decades, alongside an in-depth exploration of future challenges.

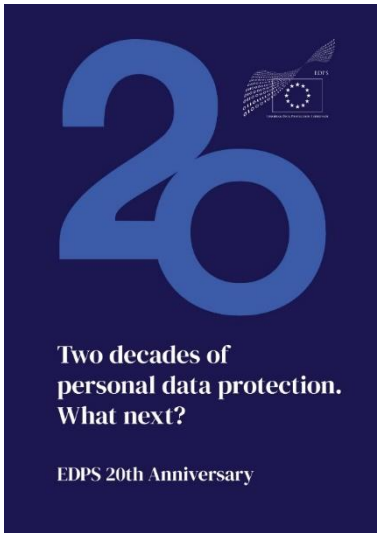
The second pillar features 20 talks with leading voices from around the world, offering unique perspectives on how data protection and privacy shape various fields, such as cybersecurity, tech, AI space and ethics.

The third pillar introduces 20 initiatives to reinforce individuals' fundamental rights and modernise the EDPS' approach to anticipate and address future challenges.

The fourth pillar is our European Data Protection Summit: Rethinking Data in a Democratic Society, that took place on 20 June 2024 in Brussels. This event was designed to foster open and dynamic discussions on the role of privacy and data protection in modern democracies, particularly in the context of increasing data collection by states, by private or public entities.

With these four pillars, we set the goal of anticipating future challenges and opportunities, equipping actors in the digital and privacy spheres with the regulatory tools needed to protect individuals' personal data. This anniversary was not just a reflection on the past but a commitment to the future.

By reinforcing our mission and adapting to evolving challenges, we reaffirm our dedication to safeguarding individuals' rights while shaping the policies and frameworks that will define data protection in the years ahead.



8.1.
Book and Timeline

To mark its 20th anniversary, the **EDPS published in June 2024 a book titled "Two Decades of Personal Data Protection. What Next?"** This publication retraces the EDPS's journey, highlighting its role in shaping the digital landscape and safeguarding privacy. More than just a historical record, the book reflects on key lessons learned and anticipates future challenges in data protection.

The book embodies the philosophy that looking back is essential to preparing for the future. It examines how we have evolved alongside European data protection laws, emphasising the institution's unique position at the intersection of legal, technological, and societal developments. The reflections included illustrate how data protection has become a pillar of the EU, influencing policies beyond its original scope and shaping debates on democracy, digital sovereignty, and fundamental rights.

The publication is not only a retrospective but also have a vision for the years ahead. It delves into regulatory milestones, the growing complexity of privacy in an interconnected world, and the EDPS' role in addressing emerging risks. With digital transformation accelerating, this publication underscores the importance of maintaining strong, independent oversight to uphold privacy rights in the face of challenges such as artificial intelligence, cross-border data flows, and evolving security concerns.

A key strength of this book lies in its contributors. The book features 20 chapters authored by a diverse group of experts, including current and former EDPS officials, legal scholars, policymakers, and professionals specialising in data protection.

These perspectives provide a comprehensive analysis of the EDPS' impact over the years and its ongoing commitment to ensuring that privacy remains a core European value.

8.2.
20 Talks

To celebrate our 20th anniversary, the **EDPS launched the "20 Talks" series**. This initiative explores the role of privacy and data protection across different sectors, bringing together experts from technology, policy, academia, and activism. The goal is to foster discussions on current challenges, ethical considerations, and the future of digital governance. By inviting diverse perspectives, the series aims to bridge the gap between Regulation, technological innovation, and fundamental rights.

The Talks cover a wide range of topics. Discussions include the risks of online fraud and identity theft, the importance of robust data protection laws in emerging digital societies, and the evolving regulatory landscape for artificial intelligence. Other sessions focus on the intersection of privacy and human rights, highlighting how data protection safeguards dignity and freedom. Speakers also discuss the responsibilities of policymakers, industry leaders, and civil society in ensuring that privacy remains a fundamental right in an increasingly digital world. The challenges of enforcing privacy laws, particularly with large technology companies, are also examined. Experts share insights on legal frameworks, compliance strategies, and the role of independent oversight bodies in holding organisations accountable.

The Series also addresses the broader implications of technological advancements. Conversations explore the ethical use of AI, the impact of data governance on international cooperation, and the role of encryption in protecting online communications. Additionally, the Talks highlight case studies and real-world examples of how privacy challenges have been addressed in different regions. The Talks emphasise the importance of integrating privacy considerations into technological development from the outset.

8.3.
20 initiatives

Turning wishes into actions and commitments, as part of our 20th anniversary, we worked on 20 initiatives to keep up with an evolving digital landscape, to thrive and lead as a modern data protection authority.

Each month, we published initiatives tackling different aspects of data protection law.



Topics worked on include, initiatives to ameliorate data protection officers' role, analysis of AI tools, enhancing cross-regulatory cooperation.

8.4.
European Data Protection Summit: Rethinking Data in a Democratic Society

On 20 June 2024, the **EDPS hosted a major conference in Brussels to celebrate its 20th anniversary. The event gathered data protection specialists, policymakers, and technology experts to reflect on the role of data protection in modern democracies**. In an era where digital information is a key asset, the Summit aimed to rethink how data can be managed while upholding fundamental rights and ensuring democratic oversight.

Throughout the day, discussions focused on the intersection between data protection, democracy, and technological change. One key topic was the relationship between democracy and the rule of law, exploring how national security policies affect privacy rights.

While state surveillance is not fully regulated under EU law, experts debated the need for greater democratic accountability to ensure both security and privacy. Another central discussion revolved around Artificial Intelligence and Data Protection, addressing the implications of the AI Act and the Digital Markets Act (DMA). Participants examined how innovation could be encouraged while safeguarding individuals' rights.





The role of public authorities in data protection was another major focus. Speakers questioned whether current legal frameworks adequately regulate how authorities handle personal data, particularly in law enforcement and governance. The debate extended to the issue of disinformation, with experts highlighting the challenges posed by social media in shaping public opinion. The Digital Services Act (DSA) was discussed as a crucial tool in addressing data misuse and online manipulation.



CHAPTER NINE

Human Resources, Budget and Administration



As an organisation, we also have to manage our resources efficiently - such as our time, employees, and finances - to be able to carry out our tasks as the data protection authority of the EU institutions, bodies, offices and agencies (EUI). The Human Resources, Budget and Administration unit (HRBA) also carries out these tasks for the European Data Protection Board (EDPB) as a member of the EDPS, for which we provide a Secretariat.

Progress Delivered

This chapter focuses on how we:

- **managed human and financial resources** in a sustainable way to deliver our mandate and tasks;
- invested in employees, Units and Sectors by **offering training on AI**;
- supported the creation of the AI Unit.

9.1.
Development of employees, teams and of the organization

9.1.1.
Employees development: AI training, new learning opportunities, and partnerships with EUIs

Equipping employees with the appropriate skills to work has a direct impact on the organisation's success. With the constant development of new technologies and the EDPS new obligations – like the ones provided under the AI act since August 2024 - staff members need to have access to highly specialised and up-to-date training courses.



Reflecting these needs, a new policy on the use of online learning platforms was therefore adopted in 2024 to broaden the scope of the learning offers and opportunities to EDPS teams and employees.

2024 was therefore a pivotal year to improve AI literacy. Various specialised training courses were offered to the EDPS and EDPB staff depending on their background and needs in this area as well as others.

The EDPS also continued to organise training courses allowing employees to build their skills and participate in job-shadowing programmes in other EU institutions or within the different Units and Sectors of the EDPS.

Related to this later point, the EDPS participated, for the second time, in the inter-institutional Job Shadowing Programme, a short-term exchange in which an EDPS staff member is paired up with another staff member from another EUI. This programme increases respective understanding and awareness of procedures, roles, and tasks done in the EUIs involved and vice-versa.

Job shadowing initiatives were carried out inside the EDPS and, reciprocally, EDPS staff members were able to follow best practices in the European Commission. In 2024, the EDPS welcomed five colleagues from other EUIs and sent five colleagues shadowing colleagues from the European Commission.

Given the limited budgetary, and, by extension human resources, HRBA also worked on simplifying workflows and will continue to do so in 2025. Furthermore, the results of the Staff Satisfaction Survey carried out in 2022 and analysed in 2023, were applied.

9.1.2.
Teams development: reinforcement collaboration, preparing for AI, work innovation

In January 2024, the **management team** of the EDPS also benefited from team coaching in the form of a seminar in the Jean Monnet house co-facilitated with a leadership development designer from the European School of Administration (EuSA) to foster close collaboration and a team spirit at management level as a means to incentivise staff to work together in the interest of the institution.

Likewise, several **team-building activities** were organised for the units and sectors of the organisation, benefiting working relationships, defining work missions, reinforcing the identity of the team, and setting priorities and goals.

To accompany these activities, a call for expression of interest was launched in 2024 for the hiring of internal facilitators to guide and manage team events, such as away days, walks, task forces, networking projects, as well as team-building and brainstorming exercises.

In 2024 also, the EDPS set up a working group focused on reducing the institution's carbon footprint, thus working on the comments made by the EP as Budgetary Authority in its resolution on the Discharge 2022.

Creation of the AI Unit

Significant **organisational developments** took place in September 2024, with the creation of a new AI Unit to embody our organisations evolving responsibilities under the AI Act.

To cover these responsibilities effectively, 4 members of staff were reallocated from other units to the new AI Unit. In addition, a call for expression of interest was launched in order to recruit 5 new staff members in early 2025, for a fully-fledged AI Unit.

EDPS-EDPB Away Day

On 22 October 2024, the EDPS–EDPB Away Day was organised, to **give space to staff members to participate in compassion break sessions and have conversations that matter to them**.

A large portion of the away day focused on the institution's preparative actions for AI, including the workshops for the use of AI within the institution, to define what is considered as acceptable and fair use and development of these tools.

Modernising administrative processes

In an effort to further modernise and simplify Human Resources (HR) and administrative processes, the EDPS made changes to its staff's appraisal exercise by replacing the mid-term interviews by an informal and regular feedback meeting, creating more proximity between staff and their managers.

Likewise, further steps were taken to automatise staff selection procedures, such as the use of a new application form in the EU-Survey tool, which allows a first pre-selection of candidates based on their indication about fulfilling the essential requirements for the post. The decision on the pre-selection of candidates remains with the unit needing to fill a vacant post.

9.2.
Creating a pool of talented and diverse people for data protection

9.2.1.
Recruitment

The EDPS continuously strives to bring together a diverse team of **legal** and **technical experts**, as well as other specialists in their field from all across the EU, working to shape the world of data protection. **Recruitment procedures** for both the EDPS and the EDPB are centrally managed by the HRBA unit of the EDPS.

In addition to recruiting data protection experts, the EDPS hires various other profiles to support the institution in its work faced with an increased workload. Beyond the recruitment of new staff, taking into account the staff turnover, the HRBA unit manages also short or long-term replacements. For short-term replacements, **interim staff** is hired. In 2024, 39 selection and recruitment procedures were carried out, 16 for officials, 19 for contract agents and 4 for a temporary agent.



Furthermore, the management team was reinforced by the selection of 3 Head of units. Throughout the year, the HR sector monitored and renewed contracts for contract agents and temporary agents, as well as external providers. The EDPS employs staff from 22 Member States and 2 non-Member States, thus representing a broad cultural and geographic variety of people.

9.2.2.
Our traineeship programme

Ten Blue Book **trainees** are recruited through the bluebook traineeship programme ran by the European Commission, twice a year.

Given the rising interest in this programme and the limited number of trainees assigned to the EDPS and the EDPB, the rotation system of trainees established in 2023 continues, allowing all Units and Sectors to benefit from a trainee at regular intervals.

The traineeship also allows us to spot talented profiles and recruit them to fill vacancies where they were the best candidates for the post, which is also a good return on the investment made into these trainees during their traineeship.

The HR sector of the EDPS serves as a contact point for managing the programme internally, offering support to the recruiting units throughout the selection process, supervising the allocation and distribution of quotas, for coordinating logistics and for welcoming trainees.

Our new on-boarding procedure

In 2024, the HR team continued to improve its **new on-boarding procedure started in 2023**, based on the feedback received by participants.

The newly improved on-boarding procedure includes presentations of EDPS and EDPB Units' and Sectors' tasks as well as relevant training sessions on data protection and day-to-day administrative tools and is more interactive, creating direct interactions with different services of the EDPS.

Following feedback from participants, we enhanced this programme by adding other, more hands-on training sessions and presentations to put new employees at ease in the organisation, consequentially boosting their efficiency and integration at the EDPS.

9.2.3.
Towards a talent retention and attraction strategy

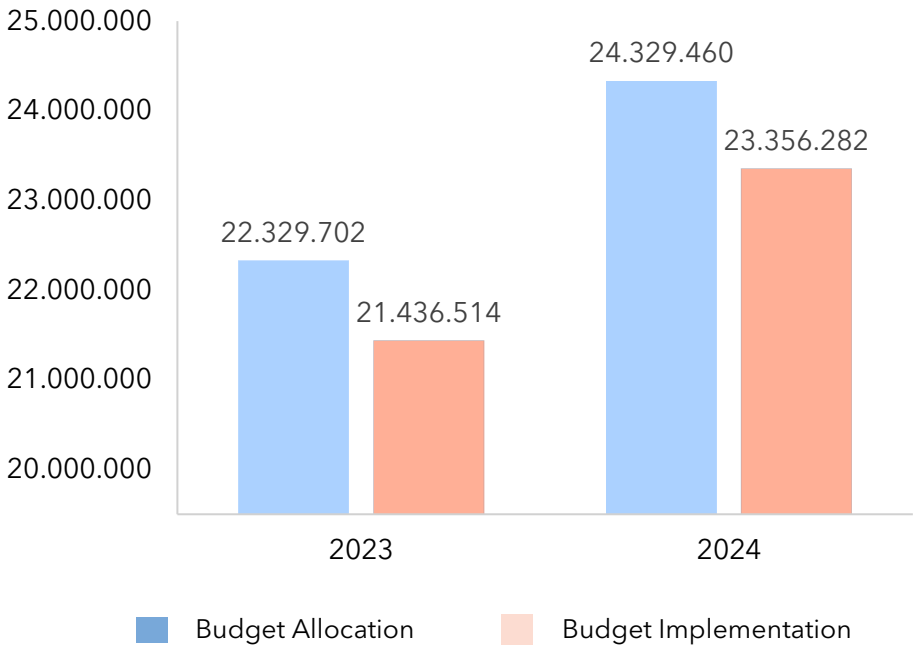
Preparing for the future, a staff retention and talent attraction strategy has been considered necessary ahead of the 2025 - 2029 mandate. As a consequence, the preparatory work was carried out in 2024 and strategy was adopted at the beginning of 2025. It comprises short/medium/long term actions.

This forward-looking document demonstrates the EDPS' commitment to maintain a solid and flexible workforce, as well as attract new talent in the evolving data protection and digital landscape.

9.3.
Budgets, expenditure and finance: managing resources for a successful organisation

9.3.1.
Allocated budget 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 staff expenditure and administrative expenditure, reflecting the new responsibilities for the EDPS decided by the lawmakers.



Budget 2023 vs 2024

9.3.2.
Budget execution

The **overall budget demonstrated a high commitment appropriation implementation rate of 96%.** This strong performance was the result of rigorous monitoring and sound financial management.

Concerning expenditures, the implementation of commitment appropriations reached 95%. Savings in this area were possible due to high number of local recruitments, a reduction on training activities through new ways of training and savings in post school childcare services.

At the same time, unanticipated fluctuations in annual inflation parameters and elevated living costs impacted staff-related expenses.

The administrative expenditure shows an exceptional implementation rate of 99%, reflecting effective resource allocation and expenditure monitoring. Despite this success, the budget line associated with expert reimbursements showed a slightly lower implementation rate of 78%, primarily due to the growing adoption of hybrid meeting formats. This shift reduced travel and associated costs, offering significant operational efficiencies while maintaining stakeholder engagement.

For the budget of the EDPB, the implementation rate reached 96%. The adoption of hybrid and virtual meeting formats for EDPB activities significantly reduced the costs associated with in-person meetings. Expenses such as travel, accommodation, venue rentals, and catering were lower than initially forecasted. Hybrid meetings also allowed broader participation from national Data Protection Authorities (DPAs) without incurring additional logistical costs, contributing to operational efficiency.

9.3.3.
Draft budget for 2025: preparing for future needs

Despite significant challenges posed by rising inflation and unexpectedly high living costs, the 2025 budget exercise was successfully completed, to ensure that the EDPS' planned priorities remain on track.

Similar to previous years, strict budgetary discipline regarding administrative expenditure and staffing across the EUIs was a key consideration in preparing the 2025 Draft Budget. However, the European Commission and the Council implemented substantial cuts in line with broader savings measures imposed on European Administration. As a result, a reassessment of priorities will be necessary, potentially leading to the modification or cancellation of certain planned initiatives for 2025.

Nevertheless, the EDPS successfully secured four additional Administrative posts (officials of the EU) and 5 Contract Agent in particular to support the evolving responsibilities and tasks under the Artificial Intelligence Act and the evolving regulatory framework on cybersecurity.



The final approved budget reflects an 11.32% increase in expenditure compared to 2024.

9.4.
Finance

The number of payment transactions (1 440) slightly increased in 2024 compared to 2023 (1 335).

This corresponds to a 7.87% increase.

However, the number of transactions is still below 2019 statistics, as some activities were impacted by the new way of working, such as the organisation of virtual or hybrid expert's meetings or events).

For 2024, 96.87% of payments have been processed on time (within 30 days).

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

The EDPS uses checklists listing the basic controls to be operated by the operational and financial agents involved in the processing of the operations. The use of Speedwell facilitates substantially the aforementioned basic controls applied on payments and commitments.

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

9.4.1.
Paperless financial workflow

Since 2020, the EDPS uses a paperless financial workflow, Speedwell. It can be seen as an extension of ABAC, an accounting system hosted by the European Commission, allowing the electronic exchanges of invoices between all actors involved in a payment process and to facilitate their verification of transaction process. This electronic workflow ensures our business continuity and allows us to fully adapt to the new hybrid working methods and improve our efficiency in processing financial transactions and the quality of the financial and accounting information. The future use of Speedwell will depend on the possibility to integrate it into SUMMA, which replaces ABAC in 2026.

9.4.2.
Procuring and contracting services

In 2024, the EDPS and EDPB launched 126 public procurement procedures, including the implementation of Framework Contracts and Service Level Agreements, for events, publications, catering, consultancy, IT services, as examples.

As always, throughout the entire public procurement procedure, the HRBA prioritises an open, fair, transparent selection and competition process and ensures that the external contractors meet high moral and ethical standards.

The use of Service-Level Agreements and Framework Contracts allows using the limited resources of the small institution in the best possible way.

9.4.3.
Managing missions

The EDPS has joined - since November 2022 - a software by the EU's Payment Management Office (PMO) to collaboratively work on the management of missions and offer support to colleagues for claims concerning their mission expenses. The PMO verifies the declaration of expenses against financial rules and on missions. As a first line mission support and for the validation of mission requests, the EDPS maintains an in-house helpdesk in the HRBA unit.

In 2024, a new monitoring system to ensure sound financial management of the missions' budget was introduced and will be continued in 2025. This has allowed reducing the expenditure on missions.



CHAPTER TEN

Governance and Internal Compliance



The Governance and Internal Compliance Unit of the EDPS (G-IC) continued to enhance the institution's internal coordination to perform its tasks effectively, focusing on:

- records, archives and knowledge management;
- internal control;
- planning coordination;
- internal compliance with data protection obligations;
- transparency and access to documents.

Progress Delivered

This chapter focuses on how the EDPS strives to build synergies, stay sharp, organised and accountable for its actions.

Check how we:

- **managed our records**, archives and knowledge;
- **digitalised our administrative processes**;
- strategically **planned our internal control** activities.

In 2024, we monitored the use of the Advanced Records System (ARES), the tool used at the EDPS to manage administrative documents; we put in place best practices, created guidelines and provided staff training to ensure for its effective use.

We also continued managing the Case Management System used for core business activities.

Since early 2024, the EDPS uses qualified electronic signatures (QES), provided by the EU Sign service from the European Commission DIGIT, which allows for fully compliant signatures of electronic documents including procurements and contracts, thus contributing to digitalisation efforts in our administrative processes.

Additionally, we initiated the appraisal of the institution's physical archives to ensure the proper application of retention periods and establish the EDPS' historical archives, in compliance with the applicable regulations on the EU institutions historical archives.

We also coordinated knowledge management activities for supporting the EDPS' decision-making process and effectiveness.

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

- the strategic planning and programming cycle;
- coordinating audits carried on selected EDPS processes;
- monitoring and reporting on related processes; and
- overseeing quality management.

In keeping with previous years, detailed information of activities carried out by the Data Protection Officer and by the Transparency Officer are provided, respectively, in chapters 11 and 12 of this Annual Report.

CHAPTER ELEVEN

Transparency and Access to Documents



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

Progress Delivered

This Chapter focuses on how the **EDPS guarantees transparency and integrity** in its actions.

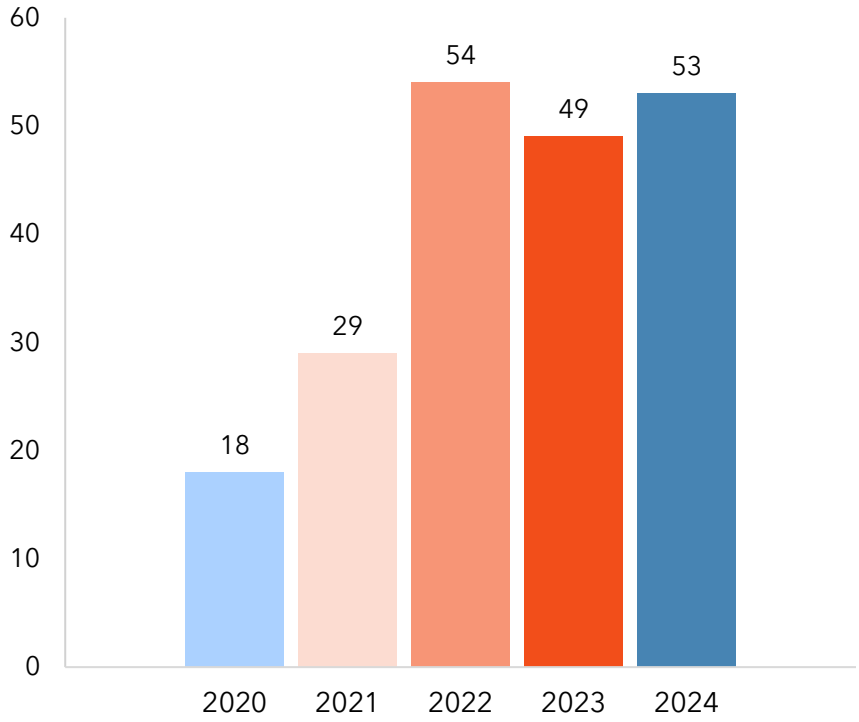
Within the EDPS, one full - time employee has been designated as Transparency officer for handling these requests.

For each request submitted to the EDPS, the Transparency officer collaborates with the relevant staff members to respond appropriately to the request.

In 2024, the **EDPS received 53 access to documents requests**.

In five of these cases (10% in 2024, same as in 2023), confirmatory applications (appeals) were also received.

In 7 cases, access to the documents falling within the scope of the request were denied as they were covered by the exceptions of Article 4(1)(a), (2) and (3) of Regulation (EC) No 1049/2001 which cover the protection of public interests related to security, as well as the protection for the purpose of inspections, investigations and audits. In all other cases where documents could be identified, they were either fully or partially disclosed to the applicant.



ATD Cases 2020-2024

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

Following up on the European Parliament's recommendations in the context of the EDPS' discharge procedures, and in line with its continued commitment to transparency, the EDPS initiated the procedure to adopt conditional and/or complementary transparency measures and their subsequent publication on the Transparency Register webpage.

CHAPTER TWELVE

The EDPS' Data Protection Officer



In 2024, the Data Protection Officer (DPO) focused on enhancing the EDPS' compliance and practical application of data protection law, whilst always keeping in mind the role and mission of the EDPS, as the data protection authority (DPA) of the EU institutions, bodies, offices and agencies (EUIs).

Progress Delivered

This chapter focuses on the work of **the EDPS' Data Protection Officer and delegated controllers to ensure accountability** of the EDPS so that it upholds the highest standards of data protection.

This section highlights how the DPO:

- monitored the EDPS' **application of data protection rules**;
- **counselled delegated controllers** in their data processing activities;
- handled, together with delegated controllers, **individuals' enquiries and complaints**.

The DPO continued to work with the EDPS' services in charge of processing personal data to ensure that the institution leads by example in upholding the highest standards of data protection.

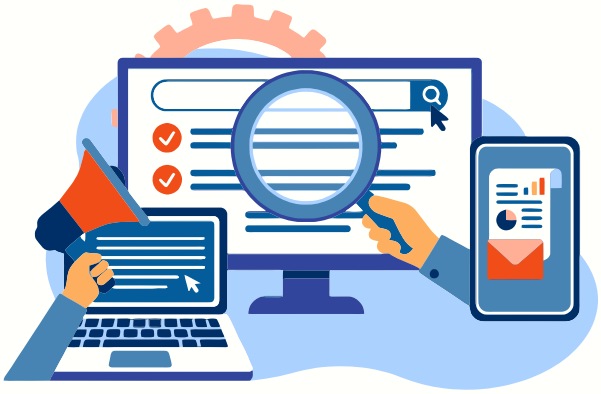
The DPO contributed to strengthening the EDPS' accountability by raising the standard of data protection compliance of both its ongoing and new personal data processing activities in its role as the DPA of EUIs.

12.1. Accountability

As the institution in charge of supervising the way EUIs handle personal data, we commit to demonstrating with transparency our compliance with data protection law and principles.

12.1.1. Monitoring the application of data protection rules

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



12.1.2. Register for processing activities

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

12.1.3. Updating data protection notices

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

12.1.4.
Ensuring the compliance of services used by EDPS

The **DPO continued the process of scrutinising the services used by the EDPS in order to clarify the responsibilities on data protection matters of the providers of these services**, and adapting, where appropriate, contractual clauses governing this collaboration. This is particularly relevant when the EDPS uses external contractors for media services, event planning, communication tools or information security, for example.

Likewise, the EDPS, as controller, continued its search and exploration of alternative options to using large-scale providers, in the context of the EU's "digital sovereignty", as per its Strategy 2020-2024.

12.1.5.
Assessing data protection risks

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

12.2.
Advising the EDPS

The DPO continued to **advise and work closely with services in charge of processing personal data to ensure the EDPS' compliance with data protection law and practice**.



In particular, the DPO counselled the EDPS on the data protection compliance of new services that the EDPS was considering to use, such as in the fields of human resources, IT, and communication.

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

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

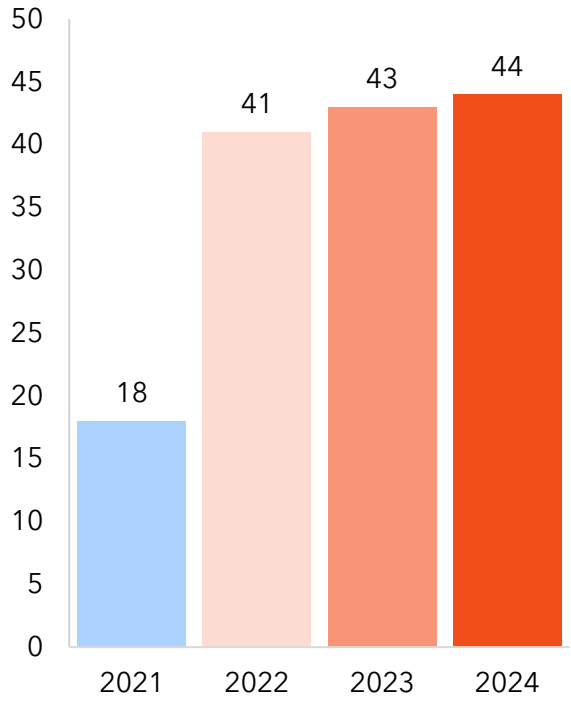
12.3. Enquires and complaints

The **EDPS' DPO assists the controller to respond to enquiries and complaints made by individuals** whose personal data has been or is processed by the institution.

12.3.1. Enquiries

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

- 19 access requests
- 6 information requests
- 13 erasure requests
- 2 objection requests
- 1 rectification request
- 3 consent withdrawals
- 47 inadmissible requests

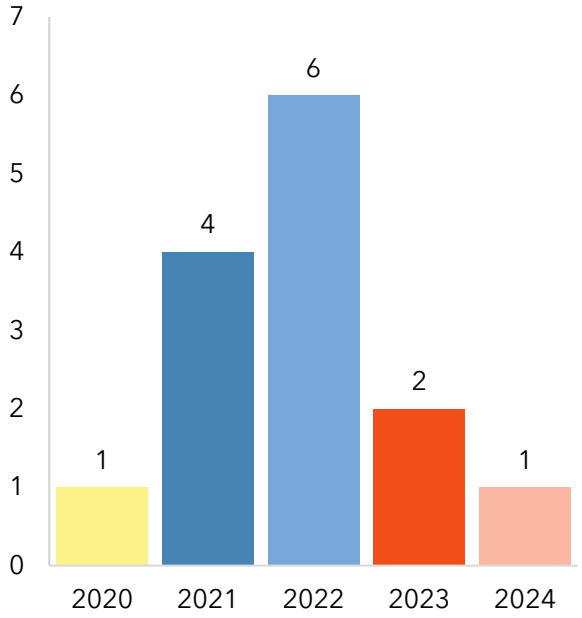


Inadmissible Data Subject requests

12.3.2. Complaints

In 2024, the EDPS, as controller, received one complaint from a citizen on the way the EDPS manages consent to cookies on its corporate website.

The citizen concerned alleged that the EDPS did not provide the option to refuse consent to cookies. The complaint was informed that users are given the option to refuse optional cookies, in accordance with the legal provisions and practice.



Complaints

12.4. Raising awareness about data protection

In 2024, the DPO delivered a number of training sessions and carried out other activities within the institution to raise awareness about data protection. Data protection is part of the training that new EDPS colleagues receive upon joining the institution; it is a module that is updated regularly to take into account the latest developments in the field, including the most recent internal rules and procedures of the EDPS.

To raise awareness on data protection, the DPO also organised an artistic competition for Data Protection Day 2024, giving the opportunity to EDPS staff to pair up their expertise in data protection and artistic talents.

This activity, held every year, is appreciated by colleagues. In 2024, a variety of fascinating entries, focusing primarily on the interplay between data protection and AI, were presented.

This competition is also a way to reinforce collegiality between the EDPS staff, and to discuss data protection in a unique manner.

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

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

The DPO partook in the DPOs biannual meetings and the EDPS' biannual meetings with the network of DPOs in June and November 2024. The meetings focused on topical matters, such as Data Protection Impact Assessments (DPIAs), Artificial Intelligence (AI) and data protection, DPO position, individuals' requests.

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





Publications Office
of the European Union

EDPS