



EDPS

EUROPEAN
DATA PROTECTION
SUPERVISOR



ANNUAL REPORT

2023



An executive summary of the Annual Report 2023, which gives an overview of the key developments in EDPS activities in 2023, 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.

Waterford, Ireland – Brussels, Belgium: Trilateral Research Ltd, Vrije Universiteit Brussel, 2024

© Design and Photos: Trilateral Research Ltd, 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 978-92-9242-825-9 ISSN 1830-5474 doi: 10.2804/71999 QT-AA-24-001-EN-C

PDF ISBN 978-92-9242-828-0 ISSN 1830-9585 doi: 10.2804/990699 QT-AA-24-001-EN-N

Table of contents

Foreword	1
About us	3
Looking ahead, our vision for 2024	7
Our 2023 highlights	9
Supervision and Enforcement	17
Policy and Consultation	49
Technology and Privacy	67
Communicating on data protection	86
Human, Resources, Budget, Administration	99
Governance and Internal Compliance	109
The Data Protection officer of the EDPS	111
Transparency and access to documents	116

Foreword

I have the honour of presenting the EDPS Annual Report summarising our activities of the year 2023. Looking back on our achievements, I see with pride the EDPS' adaptability to a changing world and the ability to tackle proactively the challenges of today and tomorrow.

We demonstrated these skills with the complexity of our actions in the field of Artificial Intelligence. While AI has dominated the public debate last year, the EDPS, contributed to the shaping of AI by ensuring that the fundamental rights to privacy and data protection, and by extension, its rules and principles continue to apply to any development, use and application of AI tools. It is according to these principles that we carry out our work and steer discussions at global level with fellow data protection and privacy authorities during various international fora and initiatives, such as the Roundtable of G7 Data Protection and Privacy Authorities during which we adopted a Statement on Generative AI, or the 45th Global Privacy Assembly Resolution on Generative Artificial Intelligence Systems, which the EDPS championed.

Our work did not stop there. The EDPS has been actively engaging in designing new legal frameworks for AI, particularly the EU's AI Act. To support the legislator, the EDPS issued its Final Recommendation on the AI Act aimed at ensuring that the tasks and duties of the EDPS - as the future AI Supervisor of the EU



institutions, offices, agencies and bodies - are clearly spelled out to guarantee that AI systems used and developed by them are safe and sound. I also reiterated my call for the prohibition of AI systems posing unacceptable risks to individuals. In the same vein, we issued an Opinion on draft AI liability rules.

Building on our previous contributions on the measures aimed at combatting child sexual abuse online, the EDPS organised on 23 October 2023 a seminar dedicated to the ongoing legislative work on the European Commission's Regulation Proposal on Child Sexual Abuse Material (CSAM). The seminar gathered stakeholders who over the last years have been warning the public about the risks associated with the proposal and misconceptions around its potential effectiveness. I expressed my strong conviction that the CSAM proposal would fundamentally change the internet and digital communications as we know them and mark a point of no return. I am grateful to all the participants, many of whom stressed the need to preserve the integrity of Europe's rights-based system and called for due diligence and respect for the scientific evidence displayed during the legislative process.

It is also in the spirit of addressing matters of societal impact that the EDPS used its role and power to act in the area of migration and border management. We firmly believe that the privacy of the most vulnerable is at a higher risk of being profoundly impacted. As a supervisory authority, we reached the borders - literally - by inspecting operations of Frontex at the Greek island of Lesbos in an unprecedented collaborative effort with a national data protection authority to scrutinise, on the ground, the processing of personal data of people entering the territory of the European Union.

2023 was the 19th year of the functioning of the EDPS. When we will be sharing this report, we will be already 20 years old. We very much invite you to join our celebrations for the year to come, hoping you might find what we prepared on this occasion as inspiring and thought-provoking. Thank you for being with us.



Wojciech Wiewiórowski
European Data Protection Supervisor

CHAPTER ONE

About us



1.1.

The EDPS

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.

Our mission

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



"Together our goal is to protect people's data"

- W. Wiewiórowski

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.

What we do

We have four 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 and initiatives related to data protection.
- **Technology and Privacy:** Monitoring and assessing technological developments impacting the protection of personal data. We oversee that the systems supporting the processing of personal data by EUIs implement adequate safeguards to ensure compliance with data protection rules. We implement the digital transformation of the EDPS.
- **Cooperation:** Working with data protection authorities to promote consistent data protection across the EU and European Economic Area. Our main platform for cooperation with data protection authorities is the [European Data Protection Board](#), to whom we provide a secretariat and have a [Memorandum of Understanding](#) defining how we work together.

How we work

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.

In 2023, the EDPS made [organisational changes](#) to be able to continuously respond and adapt to the evolving data protection challenges that lie ahead. These changes include the appointment of the EDPS' first Secretary-General and specific sectors to address key policy areas with an impact on data protection, such as a sector to monitor the EU's Area of Freedom Security. Other sectors have been created, one to address efficiently complaints made by individuals and launch timely investigations into

the way personal data is processed by EUIs, and another to deliver comprehensive advice to EUIs on data protection matters.

The reshaping of the EDPS also saw the creation of specialised sectors in the area of Technology and Privacy, one to ensure the oversight and auditing of IT systems; another to develop and to anticipate new technologies and their impact on privacy and data protection; and a sector to develop the independent digital transformation of the institution. We have also set up a task force on Artificial Intelligence, to keep up the pace with its development.

With the aim to lead by example when protecting individuals' fundamental rights to privacy and data protection, the EDPS has developed its own legal service.

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 admonish 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.



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

Looking ahead, our vision for 2024



The year 2024 marks the [EDPS' 20th anniversary](#); two decades of protecting privacy and data protection.

With this milestone comes the inevitable need to reflect on the progress made, the mountains conquered, and lessons learned, serving as fuel to plan ahead, to tackle the challenges of tomorrow. This exercise is necessary for any institution with an ambitious mission that wishes to adapt, to keep up the pace with an ever-evolving digital landscape, in order to be able to respond adequately to protect individuals' data protection rights.

Following this dynamic, the year 2024 will be dedicated to preparing the data protection arena of tomorrow by analysing the past, present and possible future dynamics between data protection, privacy, technology, policy and other fields.

To achieve this, the EDPS has chosen to base its anniversary on four key pillars - all designed to highlight the importance and impact of data protection.

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

To inform our work as a data protection authority going forward, we must also be able to learn from others. **Our second pillar comprises 20 talks with leading voices from around the world** who share their unique perspective on how data protection and privacy shape their respective fields.

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

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

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



CHAPTER THREE

Our 2023 highlights



Pursuing our goals and ambition to build and sustain the best data protection practices within EU institutions, bodies, offices and agencies (EUIs), to shape a safer digital future for Europe, and to protect the privacy of its citizens, we have busied ourselves by delivering on our core tasks: **Supervision & Enforcement, Policy & Consultation, Technology & Privacy.**

3.1.

Supervision & Enforcement

In the realm of our supervisory and enforcement activities ([see Chapter 4](#)), we continued to monitor, guide and verify the way EUIs process individuals' personal data, ensuring that they comply with their applicable data protection law, [Regulation \(EU\) 2018/1725](#), also known as the EUDPR.



Our work in this area was varied. It included issuing [15 Supervisory Opinions](#) on various issues: EUIs' draft rules to combat and prevent harassment; the envisaged processing of biometric data; the use of social media for various purposes; the controller-processor relationships; the exchange of information between different EUIs or EU Member States.

Using **our investigative powers**, we followed-up on, carried out or finalised our inspections of the way certain EUIs process personal data. In particular, this year, we enhanced our investigative processes to more effectively ascertain if EUIs have infringed applicable data protection laws.

This advancement underscores our commitment to continuously elevate the standards of our verification practices. Our ongoing or closed investigations of 2023 cover an array of subjects, including EUIs' use of IT tools and services that may involve the transfer of personal data outside the EU or European Economic Area; our ongoing investigation into the use of Microsoft 365 by EUIs, including the European Commission.

As part of **our supervisory work**, we continued to carry out audits, checking how EU data protection laws are put into practice by EUIs. Notably, we audited EPSO - the European Personal Selection Office - and the European Investment Bank. In 2023, the roles were also reversed as the EDPS was subject to an audit by the Internal Audit Service of the European Commission on the risk assessment methodology for planning audits.

Recognising the importance for individuals to be supported when they consider their personal data mismanaged by an EUI, **we addressed numerous complaints**. Observing their increase over the last year, we created a dynamic tool on the EDPS website to ramp up our efficiency in this process. This year, complaints related to individuals' right of access to their personal data, their right to erasure, data retention, to name a few examples.

Successful compliance with data protection law cannot happen without **the expertise of data protection officers of EUIs**. In their respective EUI, they help with putting data protection into practice. Capitalising on this, we redoubled our efforts to instill a strong and sustainable collaboration with them through various initiatives: our biannual EDPS-DPO meetings, DPO roundtables, the DPO Support Group and more.

On top of this, we also dedicated our expertise **to supervising the Area of Freedom, Security and Justice** (AFSJ) for which we have specific powers. This includes Europol - the EU Agency for law enforcement; Eurojust - the EU Agency for Criminal Justice Cooperation; EPPO - the European Public Prosecutor's Office and Frontex - the European Border and Coast Guard Agency.

We approached our supervision of the AFSJ as a whole, taking a holistic view, in order to exercise our supervisory powers. Yet, we also take into account the specificities of each of these bodies, offices and agencies, in terms of the nature and scope of their personal data processing operations, whenever needed and relevant.

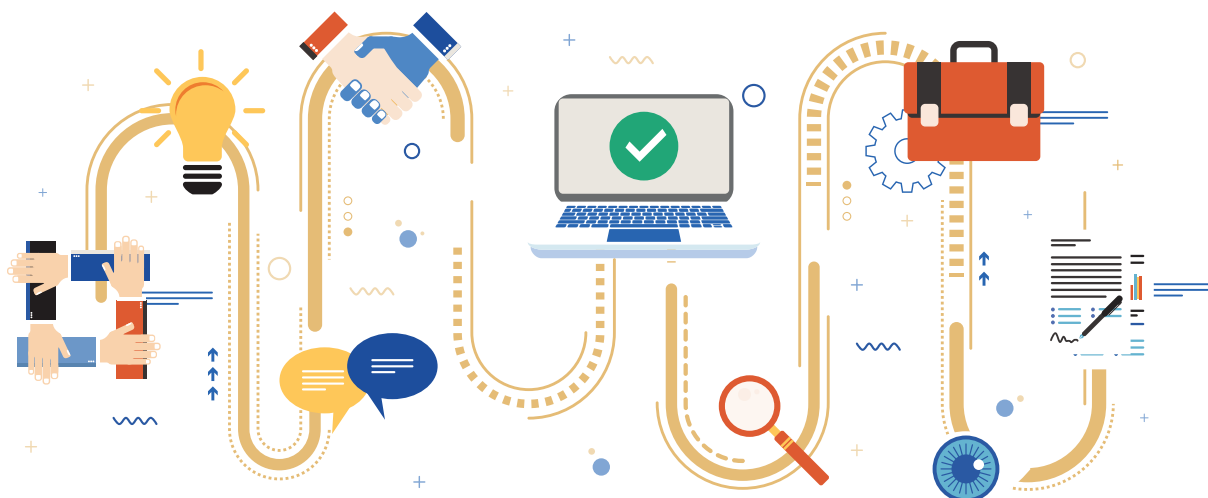
In 2023, we focused our supervisory activities over these, bodies, offices and agencies in the Area of Freedom, Security and Justice around 6 pillar-actions.

- **Preparing** for the supervision of the interoperability framework.
- **Reinforcing** our cooperation with national data protection authorities either bilaterally or through our active participation in the Coordinated Supervisory Committee, in particular to coordinate supervisory actions.
- **Scrutinising** the processing of personal data by Frontex from debriefing reports in the context of joint operations.

- **Assessing** Europol's processing of biometric data.
- **Monitoring** new ways of cooperation between Europol and EU Member States in the production of operational analysis.
- **Providing** advice on the setting up of new systems to process operational personal data by Eurojust (war crime module) and EPPO (new environment to conduct operational analysis).

3.2.

Policy & Consultation



We continued **to act as an advisor to the EU's co-legislators** - the European Commission, the European Parliament and the Council - on all new proposed legislation potentially impacting individuals' rights to privacy and personal data, we contribute to shaping a safer digital future for the EU and its citizens ([see Chapter 5](#)).

Concretely, we issued in 2023 **116 legislative consultations** - in the form of Opinions, including own-initiative Opinions, and Joint Opinions with the [European Data Protection Board](#), Formal and Informal Comments.

To this end, we invested significant time and resources in **advising the EU's co-legislators on Artificial Intelligence**, in particular the AI Act, to guarantee that the development of AI tools and systems comply with data protection law, and advocating that these tools and systems should be prohibited if they pose unacceptable risks to individuals. As an extension to this issue, we also provided advice on the AI liability rules, to ensure that individuals who suffer damages caused by AI systems used by EUIs are protected in the same way as individuals who suffer damaged caused by AI systems used by private or public sectors in other EU Member States.

We also concentrated our efforts on draft legislative proposals in the **financial sector**, notably on the Digital Euro and Financial and Payment Services, to avoid the centralisation and over processing of individuals' personal data.

Furthermore, we counselled the EU's co-legislators on **legislative proposals permeating to the policy field of justice and home affairs**, on issues related to the protection of EU citizens' rights, such as freedom of movement, as well as the EU's security, which may involve the processing of individuals' personal data.

Advocating for a **consistent approach to data protection and privacy across the EU/EEA**, we continued to cooperate with the European Data Protection Board (EDPB), of which we are a member and provide its secretariat for logistical support, on various initiatives, such as on files related to transfers of personal data outside the EU/EEA, the data processing of certain social media platforms, and more.

Championing the EU's data protection standards to become the **global standard of data protection**, we continue to collaborate closely with our international partners through different fora and platforms, such as the Global Privacy Assembly, the G7 Roundtables of data protection and privacy authorities, during which we adopted resolutions on Generative AI.

3.3.

Technology and Privacy

Complementing our core activities of monitoring the practical application of data protection law, and advising on legislative proposals with an impact on data protection law, we also anticipate the challenges of a rapidly evolving digital landscape ([see Chapter 6](#)).

In 2023, we enhanced our capabilities **to assess and prepare for upcoming and future technological trends** to measure their impact on privacy and data protection, more than ever before.



To achieve this, we monitored technological developments using a foresight-based approach, looking in particular at large language models, digital identity wallets, internet of behaviours, extended reality, deepfake detection. Our work in this area can be found in our **TechSonar reports**, the first European initiative that bridges the gap between data protection and strategic forecasting, foresight and future studies.

Whilst we attempt to predict future 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**. This year, we focused on the Central Bank Digital Currency and Explainable Artificial Intelligence.

Extending our expertise, and informing our work in return, we **collaborated with our international partners in the field of technology**. This included working closely with the EDPB on the notion of personal data, but also anonymisation, pseudonymisation of personal data, and other technical aspects, including how to interpret certain privacy-related legislation, such as the ePrivacy Directive.

With the aim to lead by example when it comes to minimising our reliance on monopoly providers of communications and software services to avoid detrimental lock in, we progressed in **our exploration and deployment of free and open source software and solutions**. This included carrying out our own IT feasibility study to identify our IT requirements, based on current and future needs; and a pathway of possible solutions to respond to these demands, such as launching our own EDPS Cloud, maintaining our alternative social media channels, EU Voice and EU Video.

We continued **overseeing systems and technology audits**, taking care of audits of large-scale IT systems, and managing personal data breaches, as well as other initiatives. As an example, we audited the Schengen Information System, focusing on information security, including security policies and management, risk mitigation, testing procedures, technical vulnerabilities, system specific legal requirements (access control management, logging and retention of logs, security incidents, specific rules for biometric data in SIS), and personal data breaches.

3.4.

Communicating data protection



As an organisation, we strive to be transparent - **explaining in clear language, accessible to all, what we are doing and why** ([see Chapter 7](#)).

To this end, over the years we have developed, and cemented, a strong online presence, primarily through **our social media channels: X (Twitter), LinkedIn, YouTube, EU Voice and EU Video, and the EDPS 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.

3.5.

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), for which we provide a Secretariat ([see Chapter 8](#)).



This year, **we accompanied the institution in its expansion and reshaping to tackle data protection challenges.**

3.6.

Key Performance Indicators 2023

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

The KPI scoreboard below contains a brief description of each KPI and the results on 31 December 2023. These results are measured against initial targets, or against the results of the previous year, used as an indicator.

In 2023, we met or surpassed - in some cases significantly - the targets set in all KPIs, except one, confirming the positive trend in implementing our strategic objectives throughout the year.

One KPI did not fully meet the set target, KPI7, concerning followers on EDPS social media account. In particular, in 2023 we have observed a reduced growth in the number of followers on our X account (ex-Twitter). This might result from a general decline in the number of people active on this social media platform.

KEY PERFORMANCE INDICATORS		RESULTS 31.12.2023	TARGET 2023
KPI 1  Internal indicator	Number of cases, incl. publications, on technology monitoring and on promoting technologies to enhance privacy and data protection organised or co-organised by the EDPS	20 cases	10 cases
KPI 2  Internal & External Indicator	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8 activities	8 activities
KPI 3  Internal Indicator	Number of cases dealt with in the context of international cooperation (GPA, CoE, OECD, GPEN, IWGDPT, Spring Conference, international organisations) for which the EDPS has provided a substantial written contribution	36 cases	5 cases
KPI 4  External Indicator	Number of files for which the EDPS acted as a lead rapporteur, rapporteur , or a member of the drafting team in the context of the EDPB	20 files	5 files
KPI 5  External Indicator	Number of Article 42 Opinions and Joint EDPS-EDPB Opinions issued in response to the European Commission's legislative consultation requests	56 Opinions	5 Opinions
KPI 6  External Indicator	Number of audits/visits carried out physically or remotely	9 audits/visits	5 different audits

KEY PERFORMANCE INDICATORS		RESULTS 31.12.2023	TARGET 2023
KPI 7  External Indicator	Number of followers on the EDPS social media accounts	X: 29 413 LinkedIn: 71 238 EUVoice: 5 906 EUVideo: 752 YouTube: 2 984 Total: 110 293	Number of followers of previous year +10%
KPI 8  Internal Indicator	Occupancy rate of establishment plan	95.65%	90%
KPI 9  Internal Indicator	Budget implementation	96%	90%

CHAPTER FOUR

Supervision and Enforcement



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 compliance with the applicable data protection law, we use 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](#); and **EPPO** - the European Public Prosecutor's Office under [Regulation \(EU\) 2017/1939](#); as well as **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 investigations and audits** to verify their compliance following an alleged infringement or complaint.
- **Cooperate with the Data Protection Officers of the EUIs** to perpetuate 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 cooperation between EU Member States, to name a few examples. ([see section 4.9](#))

4.1.

Supervisory Opinions



[Supervisory Opinions](#) are either issued on the EDPS' own-initiative or at the request of an EU institution, body, office or agency (EUI) on various data protection matters, typically on how an EUI processes individuals' personal data in its day-to-day work.

4.1.1.

Preventing and fighting harassment

We provided practical advice to the European Commission on its draft decision to prevent and fight against harassment and accompanying decision concerning the restriction of certain privacy rights of individuals in a [Supervisory Opinion](#), published on 13 October 2023.

Our recommendations focused on the possible restriction of individuals' privacy and data protection rights when their personal data is processed by the Chief Confidential Counsellor and confidential counsellors of the European Commission to prevent and fight against psychological and sexual harassment.

In its Supervisory Opinion, the EDPS points out ways to ensure better compliance with Regulation (EU) 2018/1725.

As a general rule, and in this specific context, the EDPS suggests that the data protection officers of EUIs are consulted prior to any decisions to restrict individuals' privacy and data protection rights, and to inform individuals concerned of the restrictions of their rights once the circumstances that

justify the restriction no longer apply. We further recommended that the affected individuals should be informed of their right to lodge a complaint with the EDPS, if they consider that their privacy and data protection rights are infringed upon, if the reasons that led to the restriction no longer apply.

You can read the full list of recommendations made by the EDPS in its Supervisory Opinion to the European Commission [here](#).

4.1.2.

Recording MEPs' attendance using their fingerprints

In May 2023, we followed up on the planned digitalisation of the [European Parliament's Central Attendance Register for MEPs](#), based on the use of biometric data. With this proposed new system, MEPs would scan their fingerprint onto a fingerprint reader, which would record their presence in the system with a timestamp.

We initially provided advice in 2021, when this process was first envisaged. At the time, our recommendations pointed to the lawfulness of and legal basis for processing of personal data, the processing of special categories of personal data including biometric data, and on suitable measures to safeguard individuals' personal data, amongst other parameters. Fast forward to May 2023, we checked whether our recommendations on the Central Attendance Register had been applied.

In our assessment, we found that our recommendations had been partially taken on board, some of which required further work.

For example, our remarks on the lawfulness of and legal basis for processing personal data needed additional actions to ensure a more precise definition of the legal basis to guarantee legal certainty and foreseeability for the MEPs impacted.

Another example concerned the lawfulness and necessity to process biometric data that required further justifications by the European Parliament in the roll out of the Central Attendance Register.

We raised additional concerns to address. Amongst other comments made; we called for the European Parliament to provide sufficient safeguards to protect MEPs' personal data, to apply data minimisation, and to revise their data protection notice.

4.1.3.

Social media monitoring for epidemic intelligence purposes

In a [pilot project](#), the European Centre for Disease Prevention and Control (ECDC) decided to monitor, both in a manual and automated way, certain social media platforms for epidemic intelligence purposes, in view of collecting data to identify and prevent future outbreaks of contagious diseases.

But, are the ECDC's processing operations lawful?

In [our Opinion issued on 9 November](#), we found that the ECDC did not sufficiently demonstrate that it does not process personal data, including special categories of data, like health data, in the context of its social media monitoring.

Additionally, we found that the ECDC does not have the legal basis to carry out these processing operations. The ECDC Founding Regulation, which governs how the ECDC functions, does not expressly provide a lawful ground allowing for the processing of personal data through the monitoring of publicly available information on social media for epidemic intelligence purposes.

In our Opinion, we recommended that the ECDC either modifies its Founding Regulation to foresee these types of processing operations, or, alternatively, adopts dedicated internal rules.

We also made further suggestions related to ensuring transparency for data subjects, as well as on the ECDC's data protection impact assessment and more.

Read the EDPS' Supervisory Opinion, available [here](#).

4.1.4.

Controller-processor relationships

Like every year, the EDPS receives a number of questions from EUIs on their role as controllers, and the controller-processor relationship in general, when processing personal data in their activities, when procuring or outsourcing services.

A [controller](#), or data controller, determines the purposes and means of the processing of personal data. Whilst a [processor](#), or data processor, acts on behalf of the controller. When there are several controllers and processors, they share the responsibility for these tasks, and are called joint controllers and joint processors.

The European Commission and its Executive Agencies: defining the controller and processor when using corporate tools

On [19 June 2023](#), we issued a Supervisory Opinion on the relationship between different Executive Agencies of the European Commission and the European Commission when using certain corporate tools.

Our analysis focused on helping the Agencies and the European Commission identify who were the data controller(s) and data processor(s) in this context.

We issued a number of recommendations, including advising that the Executive Agencies and the European Commission should define their respective roles as joint controllers.

Service level agreements with EU institutions: where does the responsibility for data protection matters lie?

Another example involved the [EDPS' Supervisory Opinion on the status of the European Commission's Paymaster Office \(PMO\)](#) that takes care of EUIs staff's payment of entitlements in Service Level Agreements (SLAs) signed with EUIs.

In our recommendations, issued on 19 June 2023, we advised, for example, the following.

- Service Level Agreements between the PMO and EUIs should clearly indicate that the PMO is a separate controller concerning the processing of personal data that it carries out, in the context of the provision of services to EUIs. This is the case when such services fall under its exclusive competence as well as in the context of the provision of services that are provided on demand.
- To enhance legal certainty, SLAs between PMO and EU institutions should include provisions that determine the details of the exchanges of personal data taking place in this context.
- In compliance with Regulation (EU) 2018/1725, the PMO should update its record of processing activities to reflect its role as separate controller for the processing of personal data when providing services to other EU institutions.

The Electronic Exchange of Social Security Information

We issued on 27 June 2023 a [Supervisory Opinion](#) on the role of the European Commission in the project on the Electronic Exchange of Social Security Information (EESSI).

The EESSI is a decentralised information system, which facilitates the cross-border data exchange between 32 participating countries of personal data relating to social security issues, such as occupational diseases, pension or family benefits. The Opinion confirms that the European Commission is a processor of personal data in the context of EESSI.

We concluded that the European Commission does not exercise any influence over the determination of the purposes and the means of the processing at stake. Its role is limited to processing personal data on behalf of EESSI participating countries as controllers, with the aim of providing advice concerning the functioning and maintenance of the system, and for providing technical support.

Can EU institutions send personal data to EU Member States' intelligence authorities?

In another case, we provided our advice to an EUI on whether to send personal data to EU Member States' intelligence authorities.

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

EUIs should assess the reasons brought forward by the EU Member States' intelligence authorities: whether access to certain data is proportional in light of the objectives pursued in light of the impact on individuals, for example. 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 transmitting data to recipients other than EUIs established in the EU laid out under 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.

4.2.

Investigations



In January 2023, we enhanced our investigative processes to more effectively ascertain if EUIs have infringed applicable data protection laws. This advancement underscores our commitment to continuously elevate the standards of our verification practices.

Our investigation policy now includes the following steps: opening an investigation, opening evidence-gathering meetings, followed by an onsite or remote inspection, a preliminary assessment, a hearing (optional), leading up to the EDPS' final decision and its publication, as well as a possible follow-up after [investigations](#).

When conducting investigations, we strictly comply with the principles of proportionality and fairness and apply the EDPS' core values: **impartiality, integrity, transparency and pragmatism**.

Before **opening a Formal Investigation**, the EDPS may ask an EUI to provide to the EDPS certain information. We also refer to such **requests for information** as pre-investigations. This is an information-gathering measure regarding an EUI's compliance with the applicable data protection rules. It is conducted to determine whether there is sufficient basis or evidence to warrant a formal investigation: the aim is to gather initial information, assess the credibility of allegations or suspicions, and decide whether there's enough substance to justify a more extensive and resource-intensive investigation. We may decide to start a **Formal Investigation** when we have a strong suspicion of an infringement of data protection rules by an EUI.

Complementing this, we also put in place new procedures for hearings in the context of investigations.

Before reaching an investigation's final decision, the EDPS undertakes a number of steps, such as conducting an evidence-gathering meeting, or conducting an inspection, and sending a preliminary assessment. A preliminary assessment contains the investigation's findings of fact, an initial legal assessment of those findings, including any alleged infringements of the Regulation, and envisaged corrective measures.

A hearing may then be organised at the request of the involved parties to the investigation so that they can share their observations on the EDPS' preliminary assessment before any enforcement action takes place. To this end, parties can exercise their right to be heard.

To clarify how this works, the EDPS adopted on 27 September 2023 "[Rules on the Hearing in EDPS investigations](#)". These rules cover procedural aspects of the hearing, such as questions that may be submitted to the concerned parties, how the parties can submit their observations, how confidential information is handled, and other important details.

In line with the EDPS' strategy, we focused our investigatory activities from 2020 to 2024 on **EUIs' use of information and communication technologies**, such as cloud-based ones, that also involve transfers of personal data outside of the EU/EEA.

4.2.1.

EUIs' use of IT tools: what is the impact on data protection?

A pre-investigation: an EUI's use of Trello

In 2023, we closed one **pre-investigation related to one EUI's use of the cloud service, Trello**, which we had opened in 2022.

We took note that the cloud service, Trello, had not been approved, recommended, or made available by EUI's IT services, and that the EUI's data protection officer recommended to all departments of the EUI not to use the tool.

We therefore recommended to the EUI to ensure that all of its staff are made aware that only IT tools officially approved by the EUI may be used for professional purposes. The processing of personal data involving the use of IT tools by its staff for professional purposes must also fully comply with the applicable data protection law, Regulation (EU) 2018/1725. The EUI must inform the EDPS if it decides to allow the use of the cloud service, Trello, by its staff for professional purposes.

Ongoing investigation: transfers of personal data outside the EU/EEA when using cloud services

We continued to carry out our two investigations following the Schrems II judgment, first launched in May 2021, which involve transfers of personal data outside the EU/EEA. The first investigation concerns all EUIs' transfers of personal data when they use cloud services provided by Microsoft and Amazon Web Services under the Cloud II contracts. The other investigation concerns the European Commission's use of Microsoft Office 365.

The two investigations are complex - both in terms of substance and procedure - and require significant investment of the EDPS' investigatory resources.

Following-up on an investigation: assessing data protection risks of cloud services

In 2023, we followed up on our decision of April 2022 to the European Border and Coast Guard Agency, also known as Frontex, following an investigation initiated in June 2020, on their move to the cloud, without a timely and exhaustive assessment of data protection risks and identification and implementation of appropriate mitigating measures. At the



time, we ordered Frontex to comply with Regulation (EU) 2018/1725. We therefore checked in 2023 if Frontex had fully complied with the EDPS order.

Taking into account the actions taken and planned by Frontex, we decided to close the case in line with the principle of accountability under Article 4 of Regulation (EU) 2018/1725, with the expectation that Frontex fully implements all the planned actions and takes additional measures, where necessary, following the outcome of our ongoing investigations.

EDPS INVESTIGATIONS

a step-by-step guide

EDPS investigations are a way of establishing whether EU institutions, bodies, offices and agencies (EU institutions) have breached applicable data protection rules.

1

OPENING AN INVESTIGATION

The EDPS notifies the EU institution of its formal decision to open an investigation. This includes a request for evidence. The EDPS sets a deadline by which the EU institution should reply.

2

OPENING MEETING

The EDPS can organise a meeting to explain why the EU institution is being investigated, and for the EU institution to explain complex evidence orally, if necessary.

3

EVIDENCE-GATHERING MEETING

The EDPS can organise a meeting to discuss the evidence. It can also do so at the request of the EU institution or another party that could be adversely affected by the EDPS' final decision.

4

TIME TO INSPECT

The EDPS may request an onsite or remote inspection to understand concretely how data is processed by the EU institution.

5

PRELIMINARY ASSESSMENT

The EDPS informs the parties of the facts, documents, legal assessment and corrective measures envisaged that are to be included in its final decision. This step allows the parties to share their observations on the EDPS' preliminary assessment before any enforcement action takes place.

6

HEARING

The EDPS may organise a hearing at a party's request, so that it can present its observations on the EDPS' preliminary assessment.

7

EDPS' FINAL DECISION

The EDPS' final decision determines whether the EU institution has infringed data protection rules. The final decision also includes corrective measures and the deadlines by which the EU institution is to put these in place.

8

PUBLICATION OF FINAL DECISIONS

The EDPS usually publishes final decisions of its investigations. Before doing so, the EDPS always asks parties if some elements of the final decision are to be kept confidential.

9

AFTER THE INVESTIGATION

The EDPS checks whether its corrective measures have been put in place by the EU institution. If the EU institution hasn't, the EDPS may issue a fine, or refer the matter to the Court of Justice.

If the corrective measures have been correctly put in place, the EDPS closes the case.



FOR A SUCCESSFUL INVESTIGATION PROCESS

- All steps must be documented precisely.
- EDPS staff must respect their obligations of confidentiality and professional secrecy.
- EU institutions must cooperate with the EDPS. The EDPS must respect parties' right to defend themselves. This includes the right to be heard.



edps.europa.eu



4.2.2.

Complaints-based investigations

Where appropriate, we may investigate EUIs' compliance with Regulation (EU) 2018/1725 and the [ePrivacy Directive](#), looking into issues brought to the EDPS' attention through complaints and other aspects where most common compliance issues may arise. The EDPS may in particular carry out **extended complaint-based investigations** where websites or mobile applications of EUIs are concerned.

In 2023, the EDPS carried out **5 complaint-based investigations concerning EUIs' websites** and will proceed with issuing decisions in those cases in 2024.

This year we also conducted general and specific **supervisory follow ups on personal data breaches** that EUIs had notified to the EDPS. We focus on high risk cases: data breaches that lasted a very long time or were detected very late, affected a high number of individuals, involved several EUIs, or were caused by cyber-attacks flagged by CERT-EU, or were due to serious omissions of measures in place at the EUI.

Such follow up requires the involvement of EDPS staff with both legal and technical expertise during which we decided that any further action by the EDPS is required in relation to the notified personal data breaches, such as issuing additional recommendations to the EUI concerned, conducting an audit, requesting further information or opening a formal investigation.

We have observed a steady increase in the processing of personal data by EUIs, including when carrying out their core tasks, and an enhanced procedural and technical complexity of the information systems that support them. This has an impact on the resources available in the area of supervision in the EDPS.

4.3.

Audits

As part of our supervisory work, **we carry out [audits](#) in the EUIs.**

Audits allow us to verify how data protection is applied in practice at an EU institution.

We choose to audit an EUI by taking into account a number of factors, including the results of our risk analysis, whether special categories of data are processed, the time elapsed since the last audit and whether there has been an increase in the numbers of complaints. We also ensure that we cover institutions, bodies and agencies of all sizes in our annual audit planning.

Audits or other on-site checks (for example, as part of our [investigations](#)) may also be triggered by complaints, if they require verification on the spot.



4.3.1.

The European Personal Selection Office audit

In April 2023, we conducted an audit at the European Personnel Selection Office (EPSO) on the main legal data protection aspects of remotely proctored testing using external service providers. Selection of new EU officials is the display window of the EU in relation to the external world. As a public administration in charge of dealing with the personal data of a very large number of candidates, EPSO should lead by example and show that EUIs comply with fundamental rights, including privacy and data protection, when it comes to designing new selection methods.



In this spirit, the audit was designed to ensure that EPSO:

- conduct an in-depth necessity and proportionality assessment of the use of remotely - delivered testing and the processing operations it entails;
- conduct a careful assessment of the risks raised by the use of live and automated remote proctoring, including the use of artificial intelligence, and notably by transfers of personal data to countries outside the EU/EEA;
- be in control of the whole processing, make informed choices and adapt its requirements in relation to the processor(s) accordingly;
- ensure that organisational measures are taken so that data protection principles are embedded by design.

After conducting this audit, our aim is to assist EPSO in adhering to the relevant data protection legislation for EUIs as required.

The EDPS issued its audit report in January 2024. Our general recommendation to EPSO is to assess carefully the use of fully remote testing, including the use of AI.

4.3.2.

European Investment Bank audit

In September 2023, we conducted an audit at the European Investment Bank, triggered by a number of complaints received over the past years on the exercise of individuals privacy and data protection rights. Whilst the EIB's compliance with data protection law had already improved since the complaints were submitted to us, the recommendations resulting from this audit are as diverse as the cases we looked into. Overall, our advice is geared towards making sure that EIB's practices are properly documented and that individuals are reliably and transparently informed about how their data may be processed.

4.3.3.

The EDPS as auditee

In 2023, roles were reversed. The EDPS was subject to an audit from the Internal Audit Service of the European Commission on the ‘Risk assessment methodology for the planning of EDPS audits’.

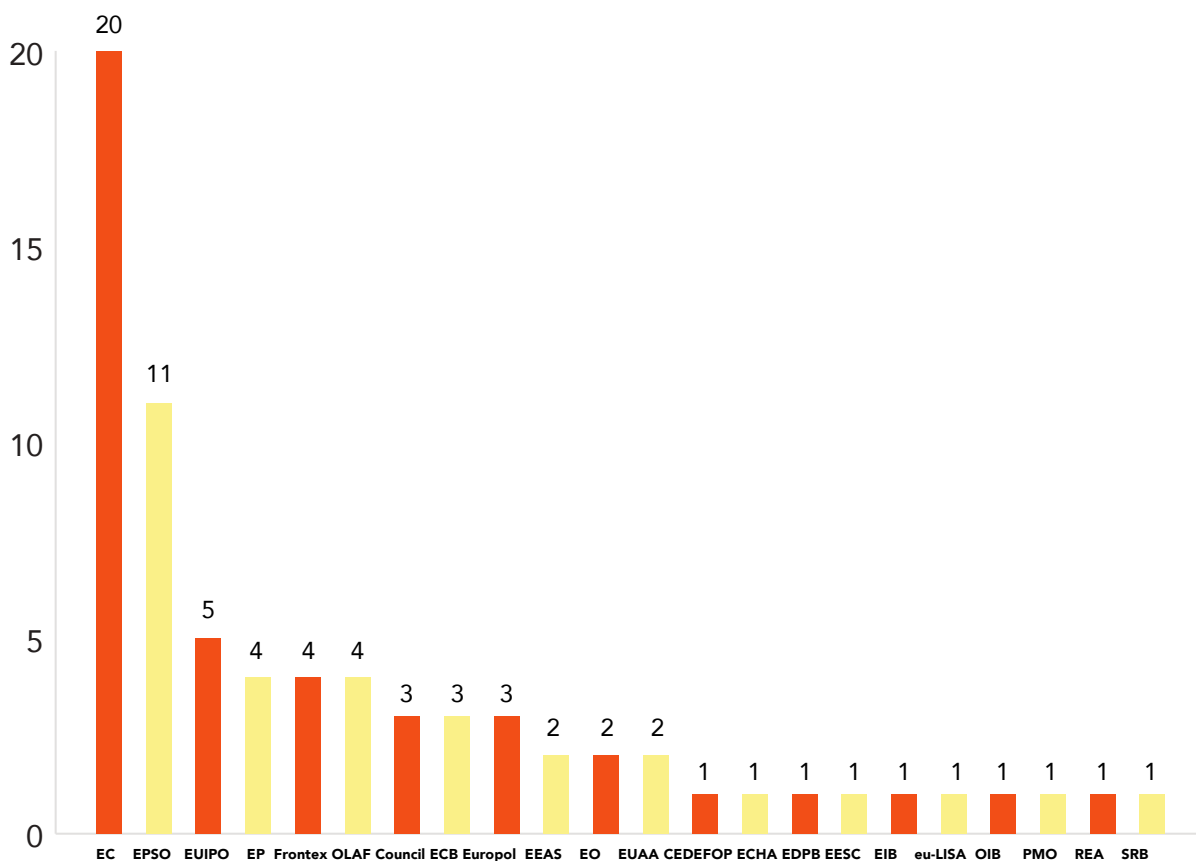
The objective of the audit was to assess whether the risk assessment methodology for the planning of EDPS audits was adequately designed and implemented.

The scope of the audit focused mainly on the procedures used to establish the annual audit plan and their practical implementation. As a result of the audit, we have prepared, in agreement with the Internal Audit Service, an action plan comprising specific actions to tackle the recommendations included in the audit report. While we have already started to plan and carry out some of the action, the action plan cover measures to be rolled out throughout 2024 and 2025.

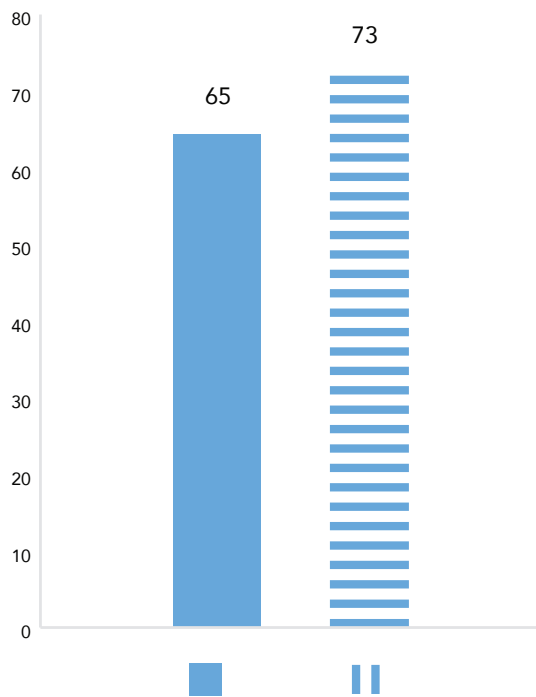
4.4.

Complaints

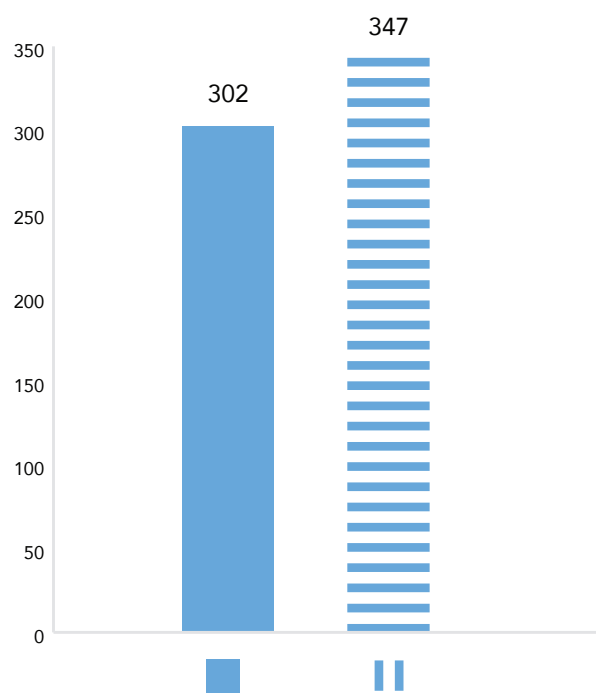
Observing **an increase in the number of complaints received by the EDPS**, and recognising the importance for individuals to be provided with rapid and comprehensive responses, we revamped our EDPS Complaints page.



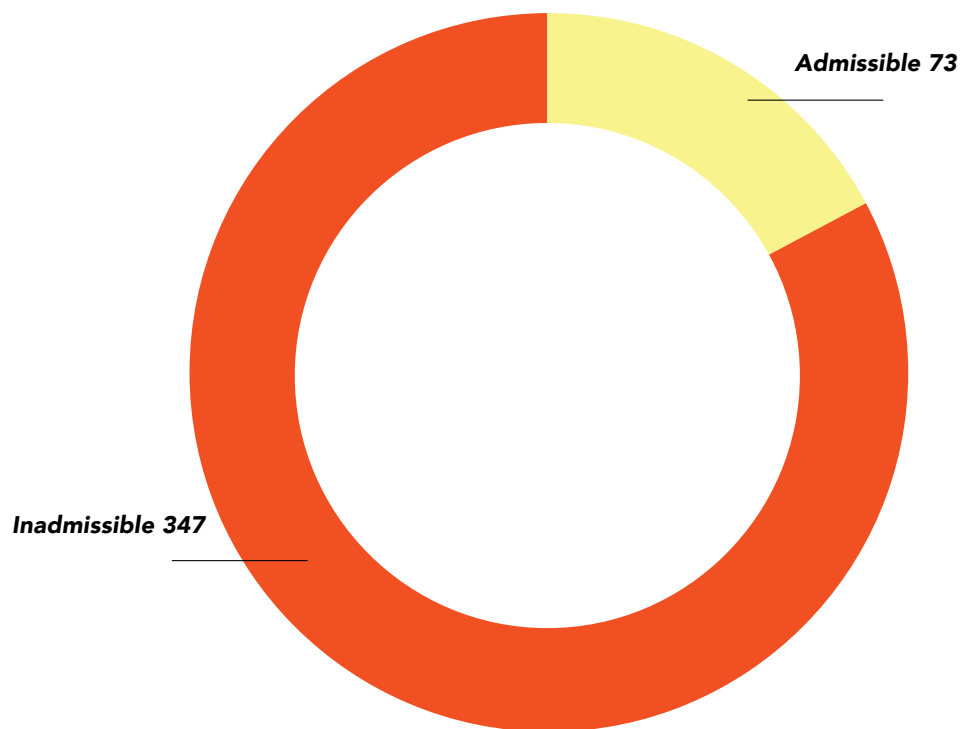
Admissible complaints per institution



Admissible 2022 Admissible 2023



Inadmissible 2022 Inadmissible 2023



Our [Complaints page](#) is now a user-friendly resource with information on what a complaint is, the scope of the EDPS' powers in this regard, tips on how to submit a complaint to the EDPS, for example.

58

Decisions on complaints during 2023

On top of this, a brand-new feature was rolled out: a dynamic questionnaire helping individuals to redirect their complaints to other competent bodies if necessary, or provide them with an appropriate response taking into account their circumstances.

With this approach, and the new online tool, we are able to satisfy individuals by providing quick and adapted responses, alleviate our workload, allowing us to focus on complaints that require our legal expertise.

The outcome of many of the complaints handled by the EDPS lead to improvements in the way EUIs protect protection of personal data, and by extension, the privacy of EU citizens.

4.4.1.

Individuals' right of access to their personal data

In 2023, we dealt with a number of complaints on the access to evaluation results in selection procedures of candidates of EUIs.

When handling these cases, we contacted the data protection officer of the EUI, referring to our interpretation of Article 17(3) of Regulation (EU) 2018/1725, which provides a detailed breakdown of an individual's right of access under the data protection law for EUIs. We therefore asked the data protection officer of the EUI concerned to provide guidance to the responsible controller.

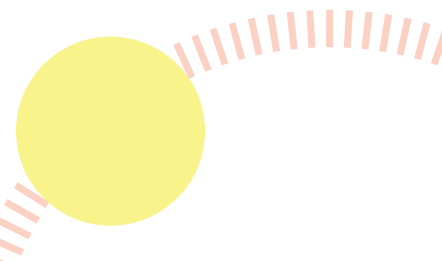
In all these cases, the complainants were granted access to a comprehensive summary of their evaluation results following our intervention. This is an efficient way of solving complaints on access requests in this context and helps reinforce data protection culture within the EUIs.

4.4.2.

Individuals' right to erasure

We also received several complaints in which individuals wanted to exercise their right to erasure of their EPSO accounts.

In these cases, we explained to the complainants that EPSO has legitimate reasons to keep accounts for a certain time and referred them to EPSO's data protection notice, which details the retention period for different categories of data. We also recommended to EPSO that they modify the data protection notice to clarify this point, and to ensure that they reply to questions from candidates about the retention of their data in a clear manner, explaining why data cannot systematically be erased upon request. Since then, we have not received any complaints on erasure of EPSO accounts.



The EDPS received a complaint in which a complainant wanted to obtain from EPSO the access to the log files regarding their EPSO profile.

In our Decision, we concluded, among others, that the log files are not the complainant's personal data and that they were therefore not entitled to have access to such information under Article 17(1)(c) of Regulation (EU) 2018/1725, which details the right of access. In response, the complainant requested that the EDPS review its position referring to a ruling of the Court of Justice (Judgment of 22 June 2023 in [Case C-579/21](#), Pankki S), that was issued shortly after the EDPS Decision.

We noted that the Court clarified in this judgment that information relating to consultation operations carried out on individuals' personal data, and the dates and purposes of those operations (i.e. logfiles), constitutes information which that person has the right to obtain from the controller under Article 15(1) of [Regulation \(EU\) 2016/679](#).

Consequently, the EDPS found that the complainant had advanced a new legal argument supporting their request for us to review our decision. After consideration, we concluded that EPSO should grant access to the complainant the available log. We based our advice on the aforementioned judgment.

4.5.

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 the EDPS 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 his tasks.

4.5.1.

Bone of contention on data retention

On 6 September 2023, the General Court issued a [Judgment](#) in favour of the EDPS concerning a case submitted by a complainant about data retention involving the Single Resolution Board ([T-200/21](#)).

In this court case, the complainant had requested a review of the EDPS' decision.



Initially, the claimant filed a complaint with us stating that the Single Resolution Board had infringed their right to erasure, their rights to object and to the restriction of the processing of their personal data, because the content of their personal file was not erased after they stopped working there and had asked for it to be erased.

In our decision, we assessed that the conditions for obtaining data erasure were not met under [Article 19\(3\) EUDPR](#), since the Single Resolution Board has the legal obligation under [Article 26 of the Staff Regulations](#) to keep the content of a complainant's personal file even after they have left service.

The complainant also put to question whether it was proportional for the Single Resolution Board to keep a staff member's personal data for 120 years after their date of birth, even if that staff member had left the service. Whilst we did not address this issue because it had no bearing on the decision we made, it is something we regularly draw EU institutions' attention to, since some follow the European Commission's Common Retention List. For example, [recently on 5 June 2023, we asked the European Commission to reconsider its retention period](#) of 100 years after the recruitment of the staff member, and to set out considerably shorter retention periods as a general rule.

We welcome the General Court's decision. When tackling complaints, our aim is to treat individuals fairly by ensuring that their fundamental rights to data protection and privacy are protected and defended. Our objective is to provide complainants with what they are entitled to expect from EU institutions under data protection law - provided they are entitled to it.

[Read the Judgment here.](#)

4.6.

Important Decisions

4.6.1.

EDPS legal action against new Europol Regulation

On 16 September 2022, we requested that the General Court of the European Union annul two provisions of the amended Europol Regulation, which came into force on 28 June 2022. In our view, these two new provisions have an impact on personal data operations carried out by Europol and in doing so seriously undermine legal certainty for individuals' personal data and interfere with the independence of the EDPS.

On 6 September 2023, the General Court found that the EDPS has no standing to bring such an action before the Court and dismissed the EDPS action for annulment as inadmissible ([T-578/22](#)). We already lodged an appeal before the Court of Justice of the European Union requesting that the General Court's order is set aside.

4.6.2.

Transfers in the use of cloud videoconferencing services

In its [Decision published on 13 July 2023](#), the EDPS found that the use of Cisco Webex videoconferencing and related services by the Court of Justice of the European Union (the Court) meets the data protection standards under Regulation 2018/1725 applicable to EUIs.

We issued this decision on the basis of the revised agreement between the Court and Cisco, which ensures that the processing of individuals' personal data occurs only in the EU/EEA. Importantly, we welcomed the Court's inclusion of technical and organisational measures to prevent the risks associated with transfers of personal data outside the EU/EEA.

We encouraged the ongoing commitments of EUIs to respect data protection law when using cloud-based services. One of the ways to achieve this is to conduct thorough assessments and analysis of any potential risks related to non-EU/EEA laws that may impact the privacy of individuals. In the coming months, we aim to further work on this matter with the Data Protection Officers of the EUIs, by providing relevant advice and guidance as their supervisory data protection authority.

4.7.

Empowering and emboldening data protection officers

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 counsel to their respective EUIs to guide them in their compliance with Regulation (EU) 2018/1725.



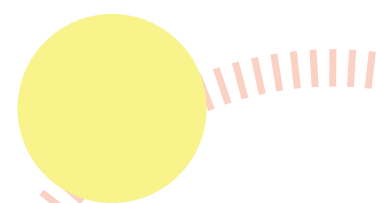
To this end, we supported and organised various initiatives to elevate compliance with data protection law, throughout the year 2023.

4.7.1.

EDPS-DPOs meetings

Twice a year, the EDPS meets with the network of DPOs of the EU institutions, bodies, offices and agencies (EUIs) to take stock of the progress made and the challenges that lie ahead in data protection.

In keeping with this tradition, over 100 DPOs and the EDPS gathered once at the EU's Intellectual Property Office in Alicante, Spain, on 12 May 2023, and once in the European Parliament in Strasbourg, France, on 30 November 2023.





During these meetings, various workshop and activities were organised - all designed to tackle the current and future data protection issues that may arise when EULs carry out their activities.

This included a workshop on the role and tasks of DPOs; the topic of Artificial Intelligence; the complex issue of transfers of personal data outside the EU/European Economic Area; the use of Open Source Software, to name a few examples.

The EDPS structures these meetings with the assistance of the DPO Support group.

4.7.2.

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 two/three months before each EDPS-DPOs meeting up until the day of the meeting.

The Group contributes to setting the agenda for the EDPS-DPOs meeting and takes an active role in the preparation of the workshop(s). With their experience, and close rapport with the DPO profession, they help the EDPS' Supervision & Enforcement Unit to decide on the topics that should be focused on during these meetings.

4.7.3.

DPOs Roundtables

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

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

To ensure fairness and equal representations of EULs, 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 EULs. This may include, transfers of personal data, access requests, the use of social media by EULs.

4.8.

Coordinated enforcement actions with other data protection authorities

In 2023, we continued our cooperation with data protection authorities within and outside the EU/EEA, extending to international fora to ensure consistent supervision and enforcement of data protection legislation. In this realm, our focus is on exchanging practical information on findings and actions taken by the EDPS and other data protection authorities.

Exemplifying our work in this area, in 2023, [we participated](#) in the [EDPB's 2023 Coordinated Enforcement Action on the role of the DPO](#). This involved, conducting an EDPS survey with the EUIs' DPOs on their responsibilities and tasks, as well as the drafting of a report on the results of the EDPS survey.

In the same vein, we participated in other coordinated enforcement actions, such as the one on the use of cloud-based services by the public sector, and on the individuals' right of access to their personal data.

This collaborative work allows the EDPS to gather a common understanding of similar issues faced by public bodies within and outside of the EU/EEA when they use similar tools to process personal data or when they carry out similar processing operations to perform similar tasks in the public interest.

4.9.

Supervising the Area of Freedom, Security and Justice

As part of our work, we also supervise the data processing operations of the following bodies, offices and agencies:

- 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).

2023	Advisory powers and authorisations				Investigative powers			Corrective powers
	Consultations (formal and informal)	Prior consultations	Audits	Operational visits	Investigations		Complaints	Use of enforcement powers
					Pre-investigations	Investigations		
Europol	4	4	1	1	1	3	2	4
Eurojust	2	2						
EPPO			1	1				
Frontex	3				3	1		
Eu-LISA								
EUAA				1				
Total AFSJ	9	6	2	3	4	4	2	4
Total per category	20				10			4

These bodies, offices and agencies are part of the Area of Freedom Security and Justice (AFSJ). AFSJ covers policy areas that range from the management of the European Union's external borders to the judicial cooperation in civil and criminal matters. It also includes asylum and immigration policies, police cooperation and the fight against crime, such as terrorism; organised crime; trafficking of human beings; drugs. With its patchwork of measures, the legal framework in the AFSJ is still fragmented. Despite these discrepancies, we are determined to enforce data protection rules consistently, in line with the rules contained in Regulation (EU) 2018/1725, in particular [Chapter IX](#).

Supervision of this area builds on the **need to actively promote justice and the rule of law as a way to promote a vision of digitalisation that enables us to value and respect all individuals**. Indeed we believe, as highlighted in our EDPS Strategy 2020 - 2024, the full potential of data should be dedicated to the good of society and with respect to human rights, dignity and the rule of law.

We therefore approach our supervision of the AFSJ as a whole, taking a holistic view, in order to exercise our supervisory powers. Yet, we also take into account the specificities of each of these bodies, offices and agencies, in terms of the nature and scope of their personal data processing operations, whenever needed and relevant.

Additionally, to enhance our supervision work in the AFSJ field, we collaborate closely with the Coordinated Supervision Committees 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 with regard to EDPS supervision of Europol, Eurojust and the EPPO..

The [Coordinated Supervision Committee \(CSC\)](#) is an EDPB structure responsible for coordinated supervision of Europol, the Schengen Information System and Eurojust. The EDPB will gradually become responsible for the supervision of the other EU large-scale IT systems. Therefore this collaborative platform ensures a consistent application of data protection rules across the EU, especially in relation to transfers of personal data outside the EU/EEA in the field of law enforcement.

In 2023, we focused our supervisory activities over the bodies, offices and agencies in the Area of Freedom, Security and Justice around 6 pillar-actions.

- **Preparing** for the supervision of the interoperability framework.
- **Reinforcing** our cooperation with national data protection authorities either bilaterally or through our active participation in the Coordinated Supervisory Committee, in particular to coordinate supervisory actions.
- **Scrutinising** the processing of personal data by Frontex from debriefing reports in the context of joint operations.
- **Assessing** Europol's processing of biometric data.
- **Monitoring** new ways of cooperation between Europol and EU Member States in the production of operational analysis.
- **Providing** advice on the setting up of new systems to process operational personal data by Eurojust (war crime module) and EPPO (new environment to conduct operational analysis).

Overall, we have concentrated our efforts on engaging regularly with the Data Protection Officers of the AFSJ Agencies and bodies to ensure a smooth collaboration in the implementation of the data protection framework.

4.9.1.

Preparing for the supervision of the interoperability framework

During the course of 2023, we stepped up our preparations for the supervision of the forthcoming AFSJ interoperability framework, focusing on deepening our cooperation with national supervisory authorities.

The framework, which is set to progressively enter into operation between 2024 and 2026, will create an interconnected ecosystem of EU border management and criminal databases, and will lead to the large-scale processing of personal data of almost every individual from non-EU/European Economic Area when they are travelling to, moving within, and exiting the EU. This data may also be processed, or retained, for years to come.

Given the considerable data protection implications of the new framework, we initiated a number of actions in 2023 in order to prepare for the multiple challenges of supervising this interoperability.

We focused on the following three priorities in this area:

- developing new approaches to auditing EU Large Scale IT Systems;
- developing an approach to supervising the use of algorithmic profiling (which will form a component of the new ETIAS and upgraded VIS);
- protecting and promoting data subject rights in the context of interoperability.

We initiated a number of parallel actions in these three key areas, aimed at deepening our knowledge, in close cooperation with national DPAs, and laying down the foundations for future supervision actions.

Interoperability study

Faced with the complexity of the framework, and to inform our work in this area, we sub-contracted academic experts from the University of Maastricht to develop, during the course of 2022 - 2023, a legal study mapping out the regulations and legislative acts applying to interoperability and highlighting the data flows in this ecosystem.

The study was delivered in July 2023 and takes the form of a tool enabling us to follow data flows, clarify interactions between systems and visualise the stakeholders who may access personal data in different locations and stages of processing. The tool is intended to aid the EDPS to identify legal gaps and ambiguities and risky processing operations, and to inform future supervisory strategies, including in cooperation with national supervisory authorities.

Fostering wider discussions to prepare supervision of interoperability

In order to further the collaborative reflection on the supervision of interoperability in AFSJ, we organised in May 2023 a panel at the CPDP Conference in Brussels titled *'Interoperability in the EU's AFSJ: preparing to supervise the "point of no return."*

The panel title alludes to the [EDPS 2018 Opinion on the interoperability regulations](#) which underscored that making large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles - particularly the principle of purpose limitation - have been interpreted in this area so far.

The panel, which brought together speakers from the EDPS, the Portuguese Data Protection Authority and Chair of the Coordinated Supervision Committee, the European Commission, and the EU Fundamental Rights Agency, aimed to address not only immediate, practical supervisory considerations of the framework, but also long-term considerations for the evolution and protection of privacy and data protection against the background of interoperability.

The panel tackled some big questions, such as:

- How can data protection authorities uphold principles of transparency and fairness, and ensure the protection of individuals' rights?
- How to supervise an ecosystem of processing operations across multiple controllers? and;
- How to audit algorithmic profiling (embedded in ETIAS: the European Travel Information and Authorisation System and VIS: the Visa Information System) to ensure it is targeted, proportionate and non-discriminatory?

4.9.2.

Audits of existing Large-Scale IT Systems

On 5-6 December 2023, the EDPS audited the Schengen Information System (SIS), the most widely used IT system for security and border management in Europe, and a critical component of the EU's upcoming interoperability framework.

The audit took place at the EU's Agency in charge of the operational management of Large-Scale IT systems, eu-LISA, in Strasbourg, France.

Since the last SIS audit, in October 2022, the Schengen Information System has been updated, with a significant number of new functionalities, as required by the SIS Regulations of 2018, including the processing of new alerts and categories of biometric data. As these new set of functionalities entered into operation in March 2023, it was important to carry out this audit to verify specific data protection and security requirements, and how these may need to evolve, or be reinforced, in light of the technical developments of the system.



This audit also allowed us to verify how current security and biometric technology frameworks are put in place at eu-LISA, and will allow us to compare and contrast with future interoperability components, such as the shared Biometric Matching Service (sBMS).

In 2023, the EDPS also audited how EU agencies make use of the EU's Large-Scale IT Systems.

In particular, the EDPS audited the process of requesting access to information stored in VIS by Europol for operational analysis purposes (querying) during an on-site inspection on 2-3 October 2023.

The possibility for Europol to query VIS is part of a broader trend involving the increase in the use of Travel Intelligence by law enforcement authorities, meaning an observed increase in the gathering of individuals' personal data who are moving from one country to another. This may also include in the future information from Passenger Name Records and (in the future) information from ETIAS.

As Europol's access to future systems such as the Entry-Exit System and ETIAS will be partially modelled on its access to VIS, this audit was key to ensure compliance with data protection obligations at an early stage, in anticipation of the rolling out of the interoperability framework.

Participation in Supervision Coordination Groups

The EDPS also supports the coordinated supervision through its active participation in Supervision Coordination Groups (SCGs). These groups are composed of representatives from the national Data Protection Authorities (DPAs) and the European Data Protection Supervisor (EDPS) to [ensure a coordinated approach to the supervision of the large-scale IT systems set up by the European Union](#).

Through the [SCGs](#), the EDPS assists with:

- **Exchanging relevant information:** to maintain a consistent level of data protection across all systems and participating authorities.
- **Examining difficulties of interpretation or application:** studying problems related to the exercise of individuals' rights to data protection.
- **Drawing up harmonised proposals for solutions** by creating shared methodologies for audits, for example.
- **Promoting awareness of data protection rights** to ensure that data subjects are aware of their rights.

Examples of practical cooperation include the common inspection plan that the VIS SCG has been working on, which can be used by data protection authorities auditing VIS and/or auditing VIS access by other authorities.

Similarly, the Eurodac SCG, which is responsible for overseeing the fingerprint database used for tracking asylum applications and individuals crossing the border irregularly, is preparing a central guidance document that all DPAs - including the EDPS - can use to audit Eurodac's access by law enforcement.

The Secretariat of these SCGs is provided by the EDPS. They meet regularly, usually twice a year, to discuss common issues regarding supervision. Following recent revisions of various regulations, the support for some of the Supervision Coordination Groups has been handed over to the European Data Protection Board (EDPB) as part of the new Coordinated Supervision Committee (see below).

More information regarding the SCGs and their activities are published on the respective webpages of the VIS, Eurodac and CIS SCGs on the EDPS website.

Cooperation under the Coordinated Supervision Committee

Cooperation within the EDPB is also organised under the Coordinated Supervision Committee (CSC), which will progressively take over and organise the coordinated supervision of all EU-large-scale databases of the interoperability framework.

In the framework of the CSC, the EDPS is participating actively in initiatives to deepen cooperation between DPAs in order to coordinate more closely supervisory activities and prepare for the rollout of the interoperability framework. Exemplifying this, a workshop was organised by Dutch DPA on 12 September 2023, which brought together around 50 representatives from national DPAs, to exchange on supervision of EU large scale IT systems in light of the forthcoming changes brought by interoperability and the new systems and upgrades.

The EDPS presented its approach to developing a strategy for the supervision of interoperability of large-scale IT systems, including actions taken so far. Discussions revealed that DPAs are encountering common challenges.

In 2023, we focused our supervision of Frontex on their involvement in data processing activities at the EU's external border in the context of so-called 'Joint Operations' between Frontex and Member States. This processing is considered particularly risky given the vulnerability of individuals concerned (migrants, asylum seekers) and its links with the exercise of other fundamental rights. Consequently, we have intensified our cooperation with national DPAs to ensure coordinated supervision where responsibilities and activities are shared at EU and national level to monitor the exchanges of personal data between Frontex and Europol.

Processing of personal data at EU borders

On 24 May 2023, we issued our [report of the audit](#) we carried out in October 2022 at Frontex's headquarters in Warsaw, Poland. The audit focused on the activities conducted by Frontex at EU borders during joint operations, in particular the interviews of individuals crossing the borders without authorisation and the further processing of the data collected in this context. We found a number of shortcomings, which led us to issue **32 recommendations**.



We expressed concerns about the way personal data is collected through interviews of individuals who have crossed the EU's external border irregularly. In light of this, we checked the way Frontex processes personal data in this context, particularly looking into whether the principle of fairness is applied. We also verify how Frontex further processes, including stores, this data, to analyse risks and to exchange them with Europol to combat migrant smuggling and traffic of human beings.

On the basis of this report, and in addition to the recommendations we provided to Frontex, we opened a pre-investigation into the collection of information during debriefing interviews in Joint Operations, followed by an onsite inspection at the EU Hotspot of Lesbos, Greece, in coordination with the Hellenic Data Protection Authority on 12-14 July 2023 to verify practices on the ground.

The onsite inspection focused on the collection of personal data in the context of Joint Operations through fingerprinting, screening and debriefing interviews of individuals crossing the EU borders without authorisation. These "Joint Operations" are carried out by Frontex staff on the territory of Member States in cooperation with the host Member State authorities.

Formal investigation: Frontex's exchange of personal data about suspects of cross-border crimes

Linked to this line of action, we were alerted by a journalist about the reporting of Non-Governmental Organisation (NGO) members in debriefing reports. We thus decided to open a pre-investigation on this matter. Upon analysing 505 debriefing reports including the term 'NGO' or 'NGOs', we noticed that there were no structural collection and further transfers from Frontex to Europol regarding personal data relating to NGOs' staff. However, we found, that such transmission of data took place in six cases out of 505. This prompted the EDPS to further investigate the lawfulness of such transmission in the context of the broader investigation we opened after the audit on Frontex's exchange of personal data about suspects of cross-border crimes with Europol.

Opinions on Frontex's internal rules on data processing

Following our opinions issued on 7 June 2022 about Frontex's internal rules for all data processing activities, we were consulted in July 2023 with new drafts decisions.

3

Consultations (formal and informal)

While Frontex has followed most of our recommendations, we are still concerned by the allocation of Frontex and EU Member States' data protection responsibilities, the processing of special categories of data, and on the role of Frontex when processing personal data to identify suspects of cross-border crime.

In that same vein, we also issued on 11 May 2023 an [Opinion](#) on the processing of personal data relating to 'contacts' and associates' (labels put on individuals) as categories of individuals processed by Frontex for the purposes of identifying individuals suspected of being involved in cross-border crimes. We concluded that this was not allowed under the current legal framework, especially since Frontex has a supporting role to Europol, Eurojust and national competent authorities in their fight against cross-border crimes.

Pre-investigation: allegations concerning the photographing of migrants by Frontex officers

1

In June 2023, the EDPS received information from an Non-Governmental Organisation (NGO) concerning a potentially unlawful data processing activity by Frontex border surveillance officers.

Investigations

The information consisted of a collection of testimonies of individuals on the move at the EU's external border, alleging that Frontex' border surveillance officers had been photographing migrants on their smartphones when intercepted without due regard to data protection obligations.

The NGO also posed a number of questions regarding Frontex' handling of its investigation into the same matter.

3

Pre-investigations

Subsequently, we opened a pre-investigation in July 2023 in order to collect information on the alleged breach and clarify our understanding of the facts.

4.9.3.

Europol

In 2023, the EDPS performed the following main actions with regard to Europol:

- issued four Supervisory Opinions in the context of the prior consultation procedure;
- issued one formal opinion on draft Management Board Decision on Art. 20(2a) of Regulation (EU) 2016/794;
- advised Europol on the modifications of their portfolio;
- launched one pre-investigation on the use by Europol of national systems for purposes of joint operational analysis which was then converted into a formal investigation;
- opened 2 additional formal investigations, one of them on the implementation of Art. 39 Regulation (EU) 2016/794 (threshold assessment);
- conducted, together with national authorities, an audit on the following topics (PNR, VIS, Implementation of Art. 18(6a) and Art. 18a Regulation (EU) 2016/794 with regard to the processing of large datasets).

4

Consultations (formal and informal)

4

Prior consultations

The EDPS' supervisory activities also focused on the processing of data about minors and of biometrics and on the new tools and new ways of doing operational analysis.

Report on Europol's Annual Inspection

3

In December 2022, we conducted an in-depth inspection at Europol on the processing of personal data of minors under 15 years old. The report on that inspection was finalised in September 2023.

Investigations

During the inspection, we examined Europol's compliance with data protection laws and the Europol Regulation (EU) 2016/794, concentrating on the data received from countries outside the EU/European Economic Area and international organisations. We assessed Europol's procedures for handling data and identifying minors' roles in organised crime. Following our inspection, we provided recommendations to enhance safeguards and ensure stricter compliance with the aforementioned Regulations, aiming to improve the protection of minors when their data is processed by Law Enforcement Authorities.

The EDPS inspection at Europol was part of a coordinated supervisory action initiated in 2020 by the Europol Cooperation Board, now overseen by the Coordinated Supervision Committee (CSC), which is established within the framework of the European Data Protection Board (EDPB).

1

Audits

This action was launched to ensure the lawful and accurate processing of personal data of minors under 15 marked as suspects in Europol systems. It involves yearly checks by national data protection authorities on the transmission of such data by EU Member States to Europol. The EDPS, as Europol's supervisory authority, also conducts checks on data transferred by countries outside the EU/EEA and international organisations, covering all contributions to Europol.

Protecting individuals' fundamental rights to privacy

1

Operational visits

In 2023, the EDPS continued to pay specific attention to the efficient application of individuals' data protection rights, including through its investigation of complaints made by individuals against Europol.

We received two new complaints against Europol in 2023, and issued four decisions following the conclusion of ongoing complaint investigations. In three out of four of those decisions, the EDPS exercised its enforcement powers and applied corrective measures.

These included:

- admonishing Europol for failure to sufficiently motivate a decision to refuse access to an individual's personal data and how it is processed;
- an order to grant (partial) access to personal data and to handle an erasure request that had incorrectly been declared inadmissible;
- two admonishments for late replies to individuals' access requests.

1

Pre-investigations

On the basis of issues revealed by checks we performed in the context of complaint investigations, we decided to open an investigation into Europol's handling of individuals' access requests.

Increased focus on the use of biometrics in law enforcement

We issued a Supervisory Opinion on a prior consultation from Europol on a new facial recognition system that the Agency may use to search a subset of images it already possesses.

We were consulted at a time when biometrics, and particularly facial recognition, are set to play a larger role in the EU's upcoming legal instruments, as evidenced in the European Commission's new proposal on migrant smuggling and the inclusion of facial images in the Prüm II system - a system for the automated exchange of data for police cooperation - as an extension to the [2008 Council Decisions 2008/615/JHA and 2008/616/JHA \(Prüm Decisions\)](#).

Facial images will thus be included in this EU police biometric data-sharing network, which already covered DNA and fingerprints.

We also provided advice to staff on the limits to biometric processing set out by Europol in its Analysis Project (AP) Portfolio. Each AP hosted at Europol is created around a specific purpose, which can be specific commodity types, specific backgrounds of criminal organisations or a specific type of criminal investigation.

The AP Portfolio documents Europol's obligations to define for each AP the specific purpose, categories of personal data and categories of individuals, participants, duration of storage and conditions for access, transfer and use of the data concerned, under Article 18(3) of the Europol Regulation.

For those APs that process biometric data, Europol provides specific justifications on why (and which) biometric data it requires for its operational analysis. The EDPS has provided continuous feedback to ensure compliance with the Europol Regulation in the context of the AP Portfolio, an important safeguard to implement the principles of purpose limitation and data minimisation.

New tools and working methods for law enforcement authorities

We were consulted on new ways of searching data stored at Europol, as well as more automated ways to share data.

4

Use of enforcement powers

We advised on a new generation of Europol's QUEST (Querying Europol SysTems) tool, called QUEST+. This is a system interface enabling the querying of both the Europol Information System (EIS) and data stored within the Analysis Projects (APs), allowing national authorities for the first time to query Europol Analysis System (EAS) from their national systems, in addition to the EIS. This enables national authorities to instantly see, without manually contacting Europol, whether there is a match ("hit") in EAS, but it does not give them direct access to the information actually stored in the system.

2

Complaints

Given the increase in automated workflows, we provided guidance on the proposed changes to the sharing of reports from the National Center for Missing & Exploited Children (NCMEC) through which Europol aims to improve the efficiency and speed of intelligence compilation. NCMEC is a private, non-profit organisation established in 1984 by the United States Congress. US law requires service providers to report what they assess as potential child sexual abuse or exploitation material disseminated through their platforms to NCMEC once they become aware of it. After determining that the report concerns an EU Member State (e.g. through the IP addresses), NCMEC makes it available to Europol who performs a preliminary analysis and disseminates it to the Member States. The NCMEC report distribution process will become more automated, with standardised, near-real-time processing of NCMEC's referrals and minimal manual intervention. This will leverage existing ICT capabilities and processes at Europol.

Amongst other recommendations, we recommended that Europol consider additional mitigation measures to address the mixed reliability of reports at the first opportunity, while the reports come in. This is to control the risk of inaccurate data being automatically extracted and imported into Europol's data environment.

Joint Operational Analysis

'*Joint operational analysis*' is a new aspect of the amended Europol Regulation, allowing EU Member States to give access to other EU Member States the information they provide to Europol for the purpose of joint operational analysis in specific criminal investigations. This new provision of the amended Europol Regulation entails the participation of different actors in the analytical activities such as the transfer of information by Europol, the visualisation of the information, the analysis itself and the drafting of a joint analytical report. Therefore, a clear allocation of the data protection responsibilities between the different actors is necessary for the efficient protection of the rights and freedoms of data subjects.

In our Opinion, we concluded that the activities required for joint operational analysis, Europol and the competent authorities of the participating EU Member States qualify as joint controllers, as they jointly define the purpose and the means of the processing. Hence, the EDPS requested that this is properly reflected in the respective rules, and that an arrangement laying down their roles and responsibilities of the participating parties is concluded.

4.9.4.

Eurojust

The EDPS is in charge of monitoring the processing of operational personal data by Eurojust and ensuring it is compliant with Regulation (EU) 2018/1727 (Eurojust Regulation) and any other Union act.

2

Consultations (formal and informal)

Core International Crimes Evidence Database

On 1 June 2022, Regulation (EU) 2022/838 entered into force providing Eurojust with an explicit legal basis to preserve, store and analyse evidence related to 'core international crimes'.

In order to execute its new mandate, Eurojust initiated the development of a new database for evidence on core international crimes, the Core International Crimes Evidence Database (CICED).

In order to ensure that the CICED complies with the EU data protection rules, the EDPS was prior consulted and issued two opinions on CICED stage 2 (secure storage) and stage 3 (analysis of structured data) focusing on data security and the data subject's right of access.

Audit Report

2

Consultations (formal and informal)

In June 2023, the EDPS finalised the report on the audit carried out at Eurojust premises in The Hague, The Netherlands. The EDPS issued **24 recommendations, focusing mostly on international transfers, security and retention of operational personal data.**

By the end of 2023, Eurojust had followed up on most of the recommendations.

4.9.5.

European Public Prosecutor's Office

EPPO has been established by the Regulation (EU) 2017/1939 (EPPO Regulation) with the competence to investigate, prosecute and bring to justice crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud. In order to execute its mandate, the EPPO processes operational personal data and in line with its regulation is subject to the supervision by the EDPS.

1

Audits

On 27 and 28 April 2023, the EDPS carried out a targeted audit at the premises of the European Public Prosecutor's Office in Luxembourg.

The audit focused on the compliance of EPPO's processing of operational personal data with the EPPO Regulation (Regulation (EU) 2017/1939), in particular with regard to the handling of data subject access requests (Articles 59 and 60 EPPO Regulation) and the functioning of the Case Analysis Tool Environment (CATE). CATE was developed in order to provide the EPPO with a secure and standardised environment for more advanced analysis of operational personal data. The EDPS was prior consulted and issued a positive opinion on CATE in October 2022.

1

Operational visits

The audit identified eleven formal findings and issued five recommendations focused on improving data subject's rights and policy on information storage in CATE.

Visit to the European Delegated Prosecutor's Office

The first operational visit to the office of a European Delegated Prosecutor took place on 16 November 2023 in Lisbon, Portugal with the representatives of the Portuguese Data Protection Authority (DPA) and the EPPO.

The EDPS team carrying out the visit was provided with examples of how the EPPO Regulation is applied in practice at national level and gained knowledge on the working environment and the challenges faced by the national European Delegated Prosecutors.

The constructive discussions on the specificities of the Portuguese national legal system and the work of the Portuguese European Delegated Prosecutor and the Portuguese DPA, helped to understand, on a more general and overarching level, how the supervisory responsibilities and the respective mandates of the EDPS and the national DPAs can be best delineated, in accordance with Article 87 of the EPPO Regulation.

Consultation: EPPO rules on the processing of personal data

On 13 April 2023, the EDPS issued an opinion on the amendment of the Rules of the European Public Prosecutor's Office concerning the processing of personal data. The first year of the EPPO functioning revealed the need to retain certain data that was considered manifestly outside of the scope of the EPPO competence for the sake of the proceedings before national courts and to identify repetitive reports. After examining EPPO's justification for the proposed storage period, the EDPS concluded that the amendment did not involve a breach of any data protection provisions of the EPPO Regulation.

4.9.6.

European Union Agency for Asylum

Following the entry into force of Regulation (EU) 2021/2303 establishing the European Union Agency for Asylum (EUAA), an operational visit was organised to the Agency's premises at the EU Hotspot Lesvos on 13 July 2023 in order to deepen the EDPS' understanding of the EUAA's functioning on the ground.

1 Operational visits

The EDPS met with EUAA representatives based in Greece and discussed the different forms of operational support provided by the Agency to the Greek national competent authorities in Lesvos within the framework of the Operational Plan 2022-2024, as well as the data processing implications for the Agency this entails.

The operational visit signals the beginning of a more structured cooperation and monitoring of this Agency's activities in order for EDPS to be better positioned to deliver guidance and supervision going forward.

CHAPTER FIVE

Policy and Consultation



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 potentially impacting 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 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 2023, the P&C Unit delivered **116 legislative consultations** - in the form of Opinions, including own-initiative Opinions, and Joint Opinions with the European Data Protection Board, Formal and Informal Comments.

Opinions are 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 also issue own-initiative Opinions as part of our [role as advisor](#) on all matters relating to the processing of personal data.

We may issue **Joint Opinions** with the European Data Protection Board (EDPB) if a legislative proposal is of particular importance for the protection of personal data. The EDPB is an independent body, of which the EDPS is a member. Established under the GDPR, the EDPB promotes cooperation between national Data Protection Authorities (DPA) of the EU/EEA to ensure the consistent application of data protection rules across the EU.

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 EU legislators before the adoption of a proposal that has an impact on data protection.

This year we provided our recommendations on a variety of matters and topics, including Artificial Intelligence, Finance, and the enforcement of the GDPR, Justice and Home Affairs, as well as others.

Evolution of Legislative consultations

	2021	2022	2023
OPINIONS	12	27	54
JOINT OPINIONS	5	4	2
FORMAL COMMENTS	76	49	26
INFORMAL COMMENTS	29	30	34
TOTAL	122	110	116

5.1.

Artificial intelligence

As the data protection authority of the EU institutions, bodies, offices and agencies (EUIs), we aim to steer the way AI is developed and applied to ensure that this technology is integrated into day-to-day lives, following a human-centred and sustainable approach, respecting privacy and data protection principles.

EDPS, the AI Supervisor for EU institutions, bodies, offices and agencies

To shape the future of AI, we delivered an [own-initiative Opinion on the AI Act](#) when the proposed Regulation entered the final stages of negotiations between the EU's co-legislators.

With this Opinion, published on 24 October 2023, we provided specific suggestions focusing on our future tasks as the authority in charge of overseeing AI systems in the EUIs.

We took the opportunity to reinstate our call, collectively made with the data protection authorities of the EU/EEA in the [EDPS-EDPB Joint Opinion on the AI Act](#), that it is paramount that the use of AI systems that pose unacceptable risks to individuals and their fundamental rights are prohibited.

Anticipating our designated role as notified body and market surveillance authority to assess the conformity of high-risk AI systems that are developed or deployed by EUIs, and our role as competent authority for the supervision of the provision or use of AI systems by EUIs, we requested that our role, tasks and powers are clarified in the AI Act.

Amongst our other recommendations, we welcomed and supported the establishment of the European Artificial Intelligence Office (AI Office).

AI: who is liable, and how are individuals protected if something goes wrong

Another major Opinion we delivered was on the [two proposed Directives on AI liability rules](#), on 11 October 2023.

Our remarks focused primarily on making sure that individuals who suffer damages caused by AI systems used by EUIs are protected in the same way as individuals who suffer damages caused by AI systems used by private or public actors in Member States.

In addition, we made specific remarks and recommendations to ensure a high level of protection of individuals, taking into account the specific characteristics of AI systems, such as opacity, autonomy, complexity. This included our recommendations that procedural safeguards established in one of the proposed Directives, namely the disclosure of evidence mechanism and the presumption of causal link, should apply to all cases of damages caused by an AI systems, irrespective of whether these systems are classified as high-risk or non-high risk.

We also asked the EU co-legislator to consider additional measures to further alleviate the burden of proof for victims of AI systems.



"It is my duty to ensure that the tasks and duties of the EDPS, as the future AI Supervisor of the EUIs, are clearly spelled out so that we can guarantee that the AI systems used and developed by EUIs are safe and sound."

- W. Wiewiórowski



5.2.

Finance

Bringing about a solution to streamline financial services and payments has been one of the priorities of the EU. In response to several draft legislative proposals, we issued recommendations to **ensure that personal data protection and privacy are upheld in the context of financial transactions and services.**



The Digital Euro

With the European Data Protection Board, we issued a [Joint Opinion on the proposed Regulation on the digital euro as a central bank digital currency](#) on 17 October 2023.

The digital euro aims to provide individuals with the possibility to make payments electronically, both online and offline, as an additional means of payment alongside cash.

We found that the proposed Regulation addressed many data protection aspects of the digital euro, such as providing the choice between paying with digital euros or in cash.

Our joint recommendations aimed to better ensure the highest standards of personal data protection and privacy for the future digital euro. In particular, we suggested measures to ensure that only the necessary personal data of users of the digital euro is processed, and to avoid excessive centralisation of personal data by the European Central Bank (ECB) or national central banks.

Financial and Payment Services

On 22 August 2023, we published two Opinions:

- one on the [proposal for a Regulation on a Financial Data Access Framework](#);
- one on the [proposal for a Regulation and Directive on payment services in the EU's internal market](#).

Both proposals aim to foster the sharing of data to broaden the offer of financial services and products, whilst providing individuals or organisations control over the processing of their financial data.

According to the Proposals, individuals and organisations would manage access to their financial data using dashboards provided by financial institutions. This would allow individuals concerned to monitor, restrict or grant access to their information.

To achieve this objective, we highlighted that individuals or organisations should be provided with complete, accurate and clear information on the provider of the financial service requesting access to their data. Information on the type of product, payment or service for which an individual's personal data would be used and the types of data requested should also be communicated.

We welcomed the efforts made to ensure the Proposals' consistency with the [General Data Protection Regulation](#) (GDPR). At the same time, both Proposals should clarify that the granting of 'permissions' to access financial data does not equate to giving consent under the GDPR. All processing of personal data following a request to access an individual's financial data must have an appropriate legal basis under the GDPR.

5.3.

GDPR enforcement

On 19 September 2023, the EDPS and the EDPB adopted a [Joint Opinion on the European Commission's Proposal for a Regulation on additional procedural rules for the enforcement of the GDPR](#).

This proposal aims to ensure the timely completion of investigations and the delivery of swift remedies for individuals in cross-border cases, by harmonising a number of procedural differences across the EU and streamlining the cross-border cooperation procedure. The proposal follows a **wish list** sent by the EDPB to the European Commission in October 2022.

In our Joint Opinion, we calibrated our advice to further improve the future legislation and, in particular, to foster timely resolution of cross-border cases, and to ensure that procedural rights of complainants and parties under investigation are respected, whilst keeping in mind constraints inherent in the GDPR enforcement model.



We called on the EU's co-legislators to use this opportunity to address practical obstacles to efficient cooperation between national data protection authorities and the EDPS.

5.4.

Justice and Home Affairs

Justice and Home Affairs is a policy field in which we routinely provide advice and recommendations. Issues related to the protection of EU citizens' rights, such as freedom of movement as well as the EU's security, often involve the processing of individuals' personal data, including sensitive information. While our main goal is to protect the rights of individuals, we approach each consultation with careful consideration of all issues at stake.

5.4.1.

Exchanging personal data to combat crime

We continued to provide counsel to the EU's co-legislators on rules governing some of its International Agreements with countries outside the EU involving the exchange of personal data to combat crime.

Our aim in these circumstances is to ensure that data protection safeguards are put in place to ensure that individuals' personal data is protected according to EU standards.

International Agreements with 5 countries in Latin America

On 4 May 2023, we issued [5 Opinions on international agreements](#) between Europol, the EU Agency for Law Enforcement and the competent authorities of Ecuador, Brazil, Peru, Bolivia and Mexico, to fight serious crime and terrorism.

Amongst our recommendations, we advised that these future International Agreements explicitly list the criminal offenses and purposes, for which individuals' personal data may be exchanged.

We advocated for the International Agreements to provide for a periodic review of the time during which transferred personal data is stored, and to put in place appropriate measures to ensure that these time periods are respected. We also noted that additional safeguards are put in place for special categories of data (such as personal data revealing ethnic origin or sexual orientation), as well as in the case of automated processing.

The EDPS also recommends that the future International Agreements explicitly exclude transfers of personal data that has been obtained in violation of human rights.

Finally, we underlined the crucial importance of the control by independent authorities in charge of overseeing the transfers of personal data in the context of these International Agreements, and that they are equipped with effective powers and appropriate tools.

Judicial cooperation with Armenia on criminal matters

In the same vein, we issued [an opinion on the signing and conclusion of the Agreement between the EU and Armenia on their cooperation between Eurojust and the competent authorities for judicial cooperation in criminal matters of Armenia](#), on 11 December 2023.

The objective of the Agreement is to enhance judicial cooperation between Eurojust - the EU agency for Criminal Justice Cooperation - and the competent authorities of Armenia by allowing the transfer of personal data to support and strengthen their cooperation in investigating and prosecuting serious crime,



in particular organised crime and terrorism, while ensuring appropriate safeguards with respect to fundamental rights and freedoms of individuals, including privacy and the protection of personal data.

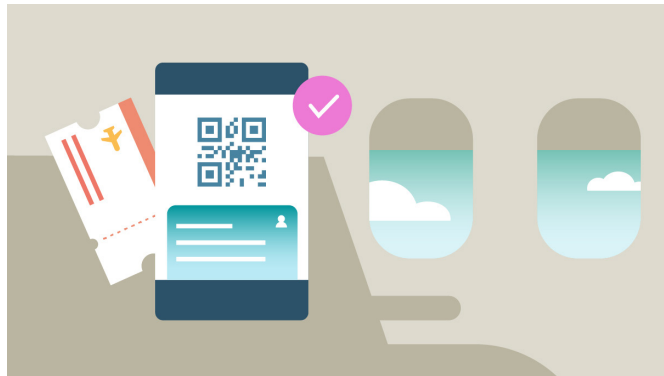
We also provided some additional recommendations on the following matters: onward transfers of personal data; right to erasure of personal data; and the review and evaluation of the future Agreement.

5.4.2.

Personal data of air passengers

One of the recurrent topics we provided advice on is on the transfer and exchange of Passenger Name Record Data (PNR): personal information about passengers travelling by plane.

In this area, we issued three Opinions on the Agreements on the [transfer of PNR data](#) between the EU and the Schengen-member states of Norway, Iceland and Switzerland.



The aim of these future agreements is to enable these three countries to lawfully receive PNR data from the EU Member States. The designated competent authority of these countries will use this data to ensure the security of the individuals moving within a common area without internal border controls, whilst also ensuring the protection of personal data concerning those individuals.

In our Opinions, we recall the specific legal situation of Schengen countries, which, pursuant to their Schengen Association Agreements with the EU, are bound by the EU acts which constitute a development of the common Schengen rules applied by EU Member States, including the rules on data protection in the field of criminal justice and law enforcement.

We also made two specific recommendations:

- to align the list of special categories of personal data, such as biometric data, to be processed in the context of Agreements with the respective provisions of the GDPR and Directive (EU) 2016/680;
- to introduce the legal possibility to suspend the Agreements in case of breaches of its provisions, as well as providing the possibility to terminate it if the non-compliance is serious and persistent.

5.4.3.

Combatting corruption

Corruption is an endemic phenomenon that takes multiple shapes and forms and may affect almost all spheres and aspects of public life. It is highly damaging to society, to the economy and to individuals.

To help combat this, we issued an [Opinion on the proposed Directive on combatting corruption](#) on 28 June 2023, in which we highlighted that the fight against corruption and the protection of fundamental rights are complementary, and are not conflicting objectives.

We supported the efforts to further enhance and harmonise the legal framework on the fight against corruption in the EU.

We advised that any limitation to exercising fundamental rights and freedoms, including the rights to privacy and personal data, should be subject to the conditions set out in the Charter of Fundamental Rights, especially the principle of proportionality, meaning limited to what is strictly necessary in light of the objective pursued as per this context. This is particularly relevant when putting in place preventive measures in the fight against corruption, such as publishing online declarations of conflicts of interest and assets. On that basis, we encouraged the EU's co-legislators to establish a comprehensive legal basis under EU law for the processing of personal data that is necessary to prevent corruption.

We also consider that the Proposal should clearly define which categories of personal data and which categories of individuals may be publicly disclosed, under what circumstances, and to put in place the necessary safeguards.

5.4.4.

Large-scale IT systems and interoperability

Similar to previous years, we addressed the data protection implications of draft implementing and delegated acts dealing with the establishment and operation of large-scale IT systems and interoperability in the area of Justice and Home Affairs.

Our advice focused on IT systems and acts that would allow:

- [EU Member States to introduce information alerts in the Schengen Information System \(SIS\)](#), based on information from countries outside the EU/EEA or international organisations;
- the introduction of specific rules to distinguish between different categories of identity in SIS and to [improve the matching of individuals' identities](#);
- automated searches launched by the [Visa Information System \(VIS\)](#);
- the use of the [European Search Portal](#).

5.4.5.

Combatting child sexual abuse online

The work of the EDPS does not stop after issuing an Opinion on a particular legislative proposal. Rather, we monitor its entire lifecycle: from the adoption of the proposal by the European Commission, through the legislative deliberations and until the approval of the final text by the co-legislators. Exemplifying this, we redoubled our efforts, already started in 2020, to help bring the European Commission's Regulation Proposal on Child Sexual Abuse Material (CSAM) into compliance with EU data protection law.

The CSAM Proposal aims to prevent and combat child sexual abuse online by detecting the dissemination of child sexual abuse material and grooming.

Whilst fully supporting the objectives pursued, we organised the "[EDPS Seminar on the CSAM Proposal: the point of no return](#)", dedicated to this topic to assess the effectiveness, necessity and proportionality of the proposed measures with our multiple stakeholders on 23 November 2023.



With more than 300 people attending the event, either in-person or remotely, coming from governmental organisations, civil society, academia and industry, the seminar provided an opportunity for a detailed discussion of the main issues at stake, and to discuss alternative measures to effectively tackle child abuse and its perpetuation on the internet.

5.5.

The essence of the fundamental rights to privacy and data protection

Pursuing this approach of organising seminars as a way to both inform and advance our work on data protection, [we organised one on the essence of the fundamental rights to privacy and data protection](#), on 8 November 2023.

On the 8 November 2023, we organised a seminar on the essence of the fundamental rights to privacy and data protection. The seminar, attended by representatives of the European Court of Human Rights, the Court of Justice of the European Union, high-level experts from academia and from EU Institutions, bodies, offices and agencies, contributed to an insightful debate on an important aspect of the fundamental rights to privacy and data protection.

More specifically, the seminar focused on:

- the meaning of the 'essence' requirement in EU fundamental rights' law in general, taking into account relevant jurisprudence of the CJEU, as well as the ECHR and national courts;

- the meaning of the ‘essence’ requirement in relation to the right to the protection of personal data as fundamental rights in particular;
- possible criteria to determine when a limitation of the right to privacy or data protection be regarded as a breach of the essence requirement.

To mark the occasion, the [study on the essence of the fundamental right to personal data protection](#) was published, which was carried out at the request of the EDPS by Prof. Dr Gloria Gonzalez Fuster, Research Professor at the Vrije Universiteit Brussel (VUB)’s Faculty of Law and Criminology, and Director of the Law, Science, Technology and Society (LSTS) Research Group.

5.6.

Participating in new EU regulatory bodies and expert groups

We participated in various EU regulatory bodies and expert groups in 2023.

5.6.1.

High-level Group for the Digital Markets Act

As a member of the High Level Group (HLG) established under Article 40 of the Digital Markets Act, the EDPS has, together with the EDPB, participated in its first two meetings.

The Digital Markets Act tasks HLG members with the responsibility of providing advice and expertise to the European Commission in the areas falling within the competences to promote a consistent regulatory approach across different regulatory instruments, including the General Data Protection Regulation and ePrivacy Directive.



Upon the request of the European Commission, we provided with the EDPB a joint contribution on the topic of consumer profiling techniques under Article 15 DMA, which obliges designated gatekeepers to report these aforementioned practices.

5.6.2.

European Data Innovation Board

Both the EDPS and EDPB are members of the European Data Innovation Board (EDIB), an expert group established under Article 29 of the Data Governance Act (DGA) and chaired by the European Commission.

The tasks of the EDIB include advising and assisting the European Commission on:

- developing a consistent practice for data altruism and for the registration of data intermediation services and data altruism organisations;
- developing the European data altruism consent form which consists of individuals providing consent for their personal data to be used in the public interest;
- the prioritisation of cross-sector standards for data use and sharing between emerging common European data spaces; and
- guidelines for common European data spaces.

The first inaugural meeting of the EDIB took place in December 2023.

5.7.

Cooperation with the EDPB

In addition to partaking in all plenary meetings of the EDPB, a large percentage of the work carried out by the EDPB takes place within expert subgroups, each of which covering a specific range of topics. These include key provisions of the GDPR, for which the EDPS is coordinator; as well as on international transfers, technology, and financial matters, amongst many others. In this context, we consistently played a leading role as a lead rapporteur, co-rapporteur, or a member of the drafting team.

As a member of the EDPB, we actively contributed to multiple EDPB initiatives in 2023.

In particular, taking on an active role as rapporteur on certain key EDPB files related to transfers of personal data outside the EEA under Chapter V of the GDPR; and most notably for the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework recognising an essential equivalent level of data protection as in the EU; and for the Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023.

In addition, we followed closely the activities of the EDPB under the consistency mechanism under Chapter VII of the GDPR that led to the adoption of the [Binding decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service \(Art. 65 GDPR\)](#); the [Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited \(Art. 65 GDPR\)](#); and the [Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd \(Art. 66\(2\) GDPR\)](#).

The EDPS also acted as lead rapporteur on various EDPB guidelines and documents adopted in 2023, such as for instance for the Targeted update of [Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority](#) (after public consultation) and for the EDPB letter in response to the European Commission regarding the cookie pledge voluntary initiative.

The EDPS also provided significant input for the [Guidelines 01/2023 on Article 37 Law Enforcement Directive](#); the Contribution of the EDPB to the report on the application of the GDPR under Article 97 or for the EDPB best practices for the organisation of EDPB Plenary meetings.

Lastly, we supported the creation of a taskforce on the interplay between data protection, competition and consumer protection, acting as its co-coordinator.

5.8.

Providing support to Supervision Coordinated Groups

We provided the Secretariat, including logistical support, to the Supervision Coordinated Group for the Customs Information System (CIS) and for the Supervision Coordinated Group for Eurodac - the information system for fingerprints and the Visa Information System, 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, including work on the adoption of new Eurodac and VIS Regulations.

More information regarding the SCGs and their activities are published on the respective webpages of the VIS, Eurodac and CIS SCGs on the [relevant EDPS webpage](#).

5.9.

International Cooperation

One of our goals, as highlighted in our EDPS Strategy 2020-2024, is to keep exchanging information and best practices with international organisations and interlocutors outside of the EU/EEA to elevate global standards in privacy and to tackle data protection matters.

5.9.1.

Global Privacy Assembly

Alongside other EDPS Units, the P&C Unit 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 2023 edition was hosted by the Personal Data Protection Authority of Bermuda, between 15 and 20 October.



Taking the lead on behalf of the EDPS, the P&C Unit took part in a variety of GPA working groups, including on:

- Global Frameworks and Standards
- The Digital Economy
- Data Protection and Other Rights Freedoms
- International Enforcement Cooperation- Digital Citizen and Consumer
- The role of Personal data in International Development Aid
- Data Sharing

The EDPS, jointly with the French data protection authority (CNIL), co-chairs the GPA working group on Ethics and Data Protection in AI (AIWG). The EDPS also takes part to other GPA working groups: International Enforcement Cooperation; Digital Citizen and Consumer; The Role of Personal Data Protection in International Development Aid; International Humanitarian Aid and Crisis Management; Data Sharing; etc.

GPA Resolution on Generative AI Systems

Building on previous work done at the level of the G7 DPAs Roundtable with the privacy and data protection authorities of Canada, France, Germany, Italy and Japan, United States and United Kingdom the EDPS initiated and acted as main sponsor of [a GPA resolution on generative AI systems that was adopted in 2023](#).

With this resolution, GPA members commit to and underline that data protection and privacy principles - including limits on data use, data minimisation, accuracy and transparency - and current laws in this area, apply to generative AI products and services, even if different jurisdictions continue to develop AI-specific laws and policies.

The resolution further endorses the existing data protection and privacy principles as core elements for the development, operation, and deployment of generative AI systems and provides initial guidance on how these principles apply in this specific context. Upon passing this Resolution, GPA members commit to sharing ongoing developments within their jurisdictions and within the Ethics and Data Protection in Artificial Intelligence Working Group, and to coordinate their enforcement efforts on generative AI systems.

In addition, during this 45th edition of the GPA, and among the various resolutions adopted, the EDPS acted as co-sponsor for the following resolutions:

- Resolution on Artificial Intelligence and Employment
- Resolution on Health Data and Scientific Research
- Resolution on Achieving global data protection standards
- Resolution on Privacy and Human Rights Award
- GPA Strategic Plan 2023-2025

5.9.2.

European Conference of Data Protection Authorities

The data protection authorities of EU Member States and the Council of Europe meet annually for the European Conference of Data Protection Authorities, or Spring Conference, to address issues of common interest, emergent trends and new developments relating to the rights to privacy and data protection. The Spring Conference also serves as a way to promote cooperation between the different regulatory frameworks and exchange best practices.

A delegation of the EDPS participated in the 31st edition of the European Conference of Data Protection Authorities (Spring Conference), held from 10-12 May in Budapest, Hungary.

Together with other members of the Spring Conference, we adopted a Resolution on the revision of the Rules and Procedures of the Conference, which sets out the vision and mission of the Conference and defining its rules and working methods, and a second Resolution on the need to enhance cooperation in the field of data protection and competition law.

The Spring Conference also welcomed a new member, the Supervisory Authority of San Marino.

5.9.3.

Roundtable of G7 data protection and privacy authorities

Shaping the global debate on data protection has long been one of the EDPS' priorities. Exchanging views allows for the development of common approaches on privacy, whilst taking into account the broader geopolitical contexts. It is also a chance for the EDPS to share and promote the EU's perspective, notably its standards related to data protection and privacy, on the global stage, and to build cooperation on that basis.

The EDPS, together with the EDPB, is representing the EU in the G7 Roundtable of data protection and privacy authorities gathering also data protection and privacy authorities of Canada, France, Germany, Italy, Japan, the United Kingdom and the United States of America.



This year, we participated in a Roundtable of G7 Data Protection Authorities organised in Tokyo, Japan, between 20 and 21 June 2023, during which we discussed joint actions on some of the key issues permeating to data protection. This included the topic of Generative Artificial Intelligence and the topic of Data Free Flow with Trust. Exchange of views were also held on emerging technologies, and how these can embed the principles of data protection and privacy, as well as strategies to enforce data protection rules.

During this roundtable, the G7 DPAs had the opportunity to hear from the activities of various international organisations and networks and to take stock of the work carried out in the working groups of the G7 DPAs.

The discussions led to the adoption of three documents:

- A Communiqué: https://www.ppc.go.jp/files/pdf/G7roundtable_202306_communique.pdf
- An Action Plan: https://www.ppc.go.jp/files/pdf/G7roundtable_202306_actionplan.pdf
- A Statement on Generative IA: https://www.ppc.go.jp/files/pdf/G7roundtable_202306_statement.pdf

5.9.4.

Council of Europe

We continued to support the efforts of the Council of Europe on the ongoing ratification process of this modernised Convention 108, as the sole global binding convention on the protection of personal data.

The Council of Europe's Convention for the Protection of Individuals on the Automatic Processing of Personal Data ([Convention 108](#)) is open to accession by both European and non-European countries. Convention 108 has been recently [modernised](#) to address challenges resulting from the use of new information and communication technologies and to strengthen the Convention's effective implementation. At the end of 2023, 31 States have ratified the Amending Protocol and seven ratifications are still required for the entry into force of the modernised Convention 108.

The Consultative Committee of the Convention 108 (T-PD) is responsible for interpreting provisions of the Convention 108, the first legally binding international instrument in the data protection field, and to facilitate and improve its application. The Committee meets twice a year in Strasbourg; its Bureau meets three times a year. We participate in all T-PD meetings as an observer. In this capacity, we actively contribute to the discussions and provide comments on the documents prepared by the T-PD. We also represent the Global Privacy Assembly before the T-PD.

Our role, in this respect, involves promoting a high standard of data protection and compatibility with EU data protection standards. The activities of the T-PD are diverse and concern topics of strategic impact for us, such as:

- facial recognition;
- artificial intelligence;
- oversight by 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, data protection in the context of neurosciences.

We followed actively the preparatory work undertaken for the new monitoring mechanism created with the modernisation of the Convention and that will play an important and strategic role, also creating additional tasks for the T-PD.

Additionally, we partake as a non-voting participant, part of the EU delegation, in meetings of the Committee on Artificial Intelligence (CAI), which has been tasked by the Committee of Ministers of the Council of Europe to elaborate a Convention on the development, design, and application of artificial intelligence systems, based on the Council of Europe's standards on human rights, democracy and the rule of law, and conducive to innovation. Supporting the overall objective, we have tried to contribute constructively, while at the same time sharing our concerns and suggestions to ensure a high level of protection for all individuals affected by AI systems.



5.9.5.

Organisation for Economic Co-operation and Development

The work of the Organisation for Economic Co-operation and Development (OECD) is becoming increasingly relevant for the EU and the EDPS given the potential impact of certain topics discussed on privacy. The OECD's work on data governance and privacy is carried out by the Working Party on Data Governance and Privacy in the Digital Economy (DGP), which reports to the OECD Committee on Digital Economy Policy (CDEP).

The DGP develops and promotes evidence-based policies on data governance and privacy. It is composed of delegates from the 38 member countries of the OECD, including representatives of governments and data protection authorities (or equivalent). We are therefore following the activities of the Working Party on Data Governance and Privacy (DGP), in particular on questions related to Data Free Flow with Trust, on government access to data held by private entities, on enforcement cooperation or on Privacy Enhancing Technologies.

The EDPS is also part of the Privacy Guidelines Expert Group (PGEG), following the activities of the Working Party on Artificial Intelligence Governance (AIGO).

5.9.6.

International Organisations' Workshop

One of the EDPS' priorities is **to generate and foster global partnerships in the field of data protection**.

One of the ways the EDPS pursues this goal is to co-organise, on an annual basis, workshops dedicated to data protection with International Organisations (IOW). These workshops, initiated in 2005, are an opportunity for all International Organisations to exchange their experiences and views on the most pressing issues they are facing.

Over the years, the relevance and significance of these workshops have grown consistently. This confirms the need for this platform for International Organisations to engage, share best practices and discuss common challenges, as well as increasing awareness on the importance of protecting individuals' personal data around the world.

The EDPS and INTERPOL - the International Criminal Police Organisation - co-hosted the 2023 edition of the International Organisations Workshop on data Protection - IOW 2023. The event took place on 24 and 25 October in Lyon at INTERPOL.

The IOW 2023 edition focused on trends in privacy and data protection, data transfer to and between International organisations; management of digital identities and the processing of biometric data, the use of cloud service providers; upcoming technology developments, including the field of AI; and the interplay between digital transformation and data protection.

5.9.7.

EDPS and ICO sign Memorandum of Understanding

The EDPS has fostered and formalised several partnerships with different institutions and data protection authorities over the years.

Adding to this list, we signed a Memorandum of Understanding (MoU) with the UK Information Commissioner's Office (ICO) on 9 November 2023 to reinforce our joint mission to uphold individuals' data protection and privacy rights, and to cooperate internationally to achieve this goal.

The MoU builds on the strong collaboration already established in other forums that both authorities mutually participate in, such as the Global Privacy Assembly and the G7 DPAs Roundtable.

This MoU aims to further strengthen the EDPS and ICO's joint commitment to ensure a consistent and coherent approach to the protection of individuals' rights to privacy and data protection.

5.9.8.

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

In September 2023, EDPS Supervisor and EDPS Secretary-General participated in a high-level seminar titled "Data-protection in the Western Balkans and Eastern Partnership Region", arranged by the SIGMA Programme; the Eastern Partnership Regional Fund for Public Administration; the Regional Cooperation Council and the Regional School of Public Administration.

The event gathered data protection authorities and public institutions from Albania; Armenia; Azerbaijan; Bosnia and Herzegovina; Georgia; Kosovo; Moldova; Montenegro; North-Macedonia; Serbia and Ukraine. These 11 countries shared their insights, unique perspectives, as well as the challenges and opportunities they encounter when advocating for digital rights and the protection of individuals' personal data.

We were present to share recommendations as the independent data protection authority supervising the EU institutions, bodies, offices and agencies, and as a member of the European Data Protection Board collaborating with other data protection authorities of the EU/EEA.

We highlighted the importance of having data protection authorities that work closely together, and that demonstrate flexibility to keep up with the rapidly changing digital regulatory landscape, and the increasing development of technologies impacting data protection.



***"International cooperation
in data protection: not an
option, but vital to our tasks"***

**EDPS Secretary-General,
Leonardo Cervera Navas**

CHAPTER SIX

Technology and Privacy



Anticipating the challenges of a rapidly evolving technological landscape, in 2023, the EDPS enhanced its capabilities in assessing and preparing for upcoming and future technological trends to measure their impact on privacy and data protection.

This multi-faceted task is carried out by the **EDPS' Technology and Privacy Unit (T&P)**.

Achieving this goal requires cross-dimensional work and expertise. To respond effectively, the T&P Unit has strategically structured itself into three sectors of competence.

The **Technology Monitoring and Foresight Sector** monitors technological developments using a foresight-based approach. Amongst its various activities, the sector regularly publishes TechSonar and TechDispatch reports, providing an in-depth analysis on upcoming technologies and their impact on privacy. Under its leadership, the sector also organises the Internet Privacy Engineering Network (IPEN) workshops, a platform that brings together a diverse pool of experts to discuss emerging technologies and their impact on data protection. In the same vein, the sector provides its expertise on technological issues faced by other EDPS Units, often complementing their supervisory and advisory tasks, as well as European Data Protection Board's (EDPB) subgroups and Task Forces, such as the Technology Expert Subgroup or the ChatGPT Task Force, as well as international working groups, such as the Global Privacy Assembly Working Group on Artificial Intelligence, or the International Working Group on Technologies and Data Protection (the Berlin Group).

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 responsible for managing personal data breach notifications communicated by EUIs.

6.1.

Technology Monitoring and Foresight

The accelerating speed of digital transformation is making it increasingly challenging 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 in light of data protection.

In this regard, our efforts in 2023 were fuelled by the need to ensure that from the earliest stages of conception, technologies are designed with data protection and privacy features.

Our work contributes to the overall EU foresight based approach to help Europe become more resilient and future-proof, as per our objectives set out in the first pillar of our EDPS Strategy 2020-2024.

6.1.1.

TechSonar: a look into the future of technologies

In December 2023, the EDPS published its third issue of the TechSonar initiative. The EDPS regularly publishes TechSonar reports that cover emerging technologies.

Launched in September 2021, the EDPS' TechSonar project is the first European initiative that bridges the gap between data protection and strategic forecasting, foresight, and future studies. By combining these fields, TechSonar addresses future technological challenges.

The [TechSonar report 2023-2024](#) explores five emerging technologies:

- Large language models (LLMs)
- Digital identity wallet
- Internet of behaviours
- Extended reality
- Deepfake detection

Similar to our previously issued TechSonar reports, T&P's group of experts have delved into the intricacies of each technology: diving into the positive aspects, challenges and impact they may have on individuals and their fundamental rights to privacy and to the protection of personal data.

The relevance and impact of TechSonar continues to grow. For example, for this year's issue, the EU's Joint Research Centre TIM Analytics service supported our identification of emerging technologies that could have an impact on data protection and privacy.

Cementing its success, the EDPS' TechSonar reports gained global recognition, winning the Global Privacy and Data Protection Award 2023 of the Innovation Category last October. The Global Privacy Award is delivered by the Global Privacy Assembly, a network that connects over 130 data protection and privacy authorities from all over the world. This achievement demonstrates that the EDPS' TechSonar report exemplifies a forward-thinking approach in response to potentially disruptive technological models.

6.1.2.

TechDispatch & TechDispatch talks

Whilst we attempt to predict future 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.

[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.

This year, we focused our TechDispatches on two key topics: the Central Bank Digital Currency and Explainable Artificial Intelligence.

Central Bank Digital Currency

The EU is currently in the process of designing the Digital Euro, the Central Bank Digital Currency (CBDC), and many other jurisdictions around the world are also considering or adopting CBDCs.

Being proactive, the EDPS decided to raise awareness on this type of technology, its functioning, main design options considered, as well as potential privacy issue, in its dedicated [TechDispatch review of March 2023](#).



Explainable Artificial Intelligence

In November 2023, the EDPS published a [TechDispatch on Explainable AI \(XAI\)](#). The purpose of XAI systems is to make AI's behaviour understandable to humans, by providing explanations on the underlying decision-making processes.



Our second TechDispatch issue of the year highlights some of the risks posed by opaque AI systems, and how AI can be approached differently with XAI.

In its analysis, the EDPS shines a light on the benefits that XAI may even have on data protection, and does not shy away from explaining the limits that also exist.

TechDispatch Talks: reaching out to a wider audience



Bringing the tech world and its correlation 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 dive deeper into 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.

6.1.3.

The Internet Privacy Engineering Network

In 2014, we founded the [Internet Privacy Engineering Network \(IPEN\)](#) initiative to promote and advance state-of-the-art privacy engineering with the idea of increasing awareness of the technologies that help protect personal data.

Under the IPEN initiative, we organise webinars and in-person events to bring together technology and data protection experts, such as academics, regulators, software engineers, to better understand the data protection impact of new technologies, to assess the state of the art of privacy-enhancing technologies and to support projects that build privacy into everyday tools.

This year, we organised an IPEN event on the topic of Explainable Artificial Intelligence (XAI) to explore the capacities and limitations of this technology trend. We used the outcome of this workshop to complement our work and research for the XAI TechDispatch.



6.1.4.

International cooperation in technology

The EDPS collaborates extensively with data protection authorities of the EU and European Economic Area (EU/EEA), as well as experts and actors from across the globe on technology and privacy matters, which are increasingly intertwined as the digital and regulatory landscape evolves.

Cooperating with the EDPB

As a member of the European Data Protection Board (EDPB) and as a provider of its secretariat, the EDPS supports them in various tasks.

Specifically, the T&P Unit takes an active part in assessing technologies' impact on fundamental rights when personal data is processed, in view of further harmonising the way the General Data Protection Regulation, applicable within the EU/EEA, and the Data Protection Regulation for EUIs are applied, given their similarities.

Topics on which we cooperate with the EDPB are numerous and diverse. Ranging from the very notion of personal data and the anonymisation and pseudonymisation processes of individuals' personal information, to other technical aspects, including how to interpret certain privacy-related legislation, such as the ePrivacy Directive. A big part of our focus this year was also to examine and assess data protection risks of artificial intelligence - such as generative AI and large language models.

The International Working Group on Data Protection and Technology

The EDPS, represented by the T&P Unit, remains actively involved in the International Working Group on Data Protection and Technology, or Berlin Group.

Composed of representatives of data protection supervisory authorities from across the globe, as well as independent experts from various sectors, including public authorities, private organisations, academia, and civil society, the Berlin Group identifies emerging technologies and practical advice on privacy-friendly and enhancing solutions with regard to data-related technologies and services.

This year, the EDPS took part in two Berlin Group meetings, one held in Rome, Italy, and another in Ottawa, Canada. During that time, the EDPS took leadership of the Central Bank Digital Currency paper, currently being finalised, whilst also supporting the drafting of the paper on Telemetry and Diagnostics data, adopted this year.

In 2024, the EDPS will host a meeting of the Berlin Group, in Brussels.

Global Privacy Assembly

The Global Privacy Assembly provides leadership in data protection and privacy at international level, by connecting more than 130 data protection and privacy authorities from across the world together to share their perspectives on the developments in data protection.

The GPA has developed massively over the years, establishing different focus groups, including a permanent Working Group to address the challenges of development of artificial intelligence (AI WG) in October 2018, which the EDPS co-chairs with CNIL, the French data protection authority.



As co-chair, the EDPS organises the quarterly meetings of the AI WG but also participates in the drafting of some of its deliverables. In 2023, the 45th Global Privacy Assembly, which took place in Bermuda, adopted two resolutions drafted by the AI WG: a Resolution on Artificial Intelligence and Employment and a Resolution on Generative Artificial Intelligence Systems. The EDPS led the drafting of the Resolution on Generative Artificial Intelligence Systems.

6.2. Digital Transformation

Championing the idea of minimising our reliance on monopoly providers of communications and software services to avoid detrimental lock-in, the EDPS has progressed in its exploration and deployment of free and open source software and solutions. At the same time, the EDPS strives to offer its employees a more modern workplace to support their work, while upholding the values of the EDPS in terms of data protection compliance.

Leading by example in this area, we hope to encourage EUIs to do the same.

6.2.1.

EDPS IT feasibility study

One of the steps we have taken to reach digital transformation for our institution is to launch an IT feasibility study to identify the EDPS IT requirements, based on current and future needs, and a pathway of possible solutions to respond to these demands.

As a follow up, a detailed study identifying different possible technical and organisational solutions for future EDPS IT infrastructure and applications, as well as suggestions on the improvement of the EDPS IT governance and management, were made.

To inform our study, T&P also evaluated approaches taken by similar organisations to the EDPS to help set criteria of selection for potential IT solutions.

6.2.2.

Reviewing the use and limits of current IT tools

From July to December 2023, the EDPS analysed the use of IT solutions and tools used for hosting its websites, social media channels, and other collaborative platforms, and compared them to other solutions available to the EDPS.

Weighing up the advantages and disadvantages of these IT tools, the EDPS decided to rely on the data centre of the European Commission's Directorate General for Digital Services, with whom we have signed a Memorandum of Understanding, for some of our IT tasks in the future.

IT services managed or received from the EP and the EC

The EDPS receives its basic IT services from the European Parliament's Directorate-General for Innovation and Technological Support (ITEC). This includes network connectivity, corporate workstations and environment, email and office productivity tools. Whilst we receive IT support for administrative applications, such as HR, budget and procurement applications from the European Commission's Directorate General for Digital Services (EC's DIGIT).

The T&P's Digital Transformation Sector is the single point of contact between the EDPS and these service providers, as well as with other EUIs and external service providers for IT matters. The Sector manages the relationship with these service providers, ensuring good communication and striving for interoperability between all the services provided.

In the context of the IT Feasibility Study, during 2023, the Technology and Privacy Unit invested significant efforts to strengthen its working relationship with the EC's DG DIGIT and with the EP's DG ITEC, to improve and explore different IT solutions, in line with the strategy of sharing and re-using IT solutions.

Having fast and privileged communication channels with ITEC and DIGIT mitigates the risk associated with having different service providers for basic IT tools and for the other applications.

Against this background, and to improve the efficiency of our work, we are testing other tools from the European Commission.

These include:

- **SECABC**, a framework for facilitating the exchange of address books among EUIs, including the signing and encryption certificate's public keys. The goal of this project is to overcome the interoperability problems associated to using email certificates for the secure exchange of encrypted messages amongst EUIs. SECABC is therefore a solution that allows all participating EUIs to share the public keys of their email certificates.
- The **EU Send service**, a platform allowing secure electronic exchange of documents and data between Public Administrations, EUIs, businesses. We are testing EU Send Web, in order to analyse and determine the feasibility of using it as a secure channel to exchange sensitive non-classified information with other EUIs.

6.2.3.

Building and maintaining our own services

This year, we strived to develop or use technologies that prioritise the respect for privacy and personal data protection.



The EDPS Cloud

In February 2023, we started **piloting the use of the Open Source Software Nextcloud and Collabora Online** (based on LibreOffice technology). Together, they offer the possibility to share files, send messages, make video calls, and allow collaborative drafting, in a secured cloud environment.

We negotiated the contract with an EU-based service provider to also allow access to all EUIs. The contract ensures compliance with the EU's data protection law applicable to EUIs, Regulation (EU) 2018/1725, as well as other rules specifically applicable to EUIs as an international organisation.

By procuring the Open Source Software from one single entity in the EU/EEA, the use of sub-processors is avoided. In doing so, the EDPS avoids subsequent data transfers to non-EU/EEA countries and allows for a more effective control over the processing of personal data.

Since its debut, we have worked on speeding up the capacity of the platform, enhancing users' experience by fixing bugs, making it easier to manage files, and anticipating the storage space needed for storing files.

EU Voice and EU Video

Since the launch in April 2022 of the pilot projects, EU Voice and EU Video, our alternative, decentralised, open-source and privacy-orientated social media platforms to share short posts, images and videos with our audience, we have continuously maintained and upgraded their functioning. Our work in this area focused on stabilising the platforms, bug fixing and rolling out security updates to ensure the safety of our users.

Qualified digital signatures from a trusted eIDAS provider

Shifting towards digitalisation, we procured and installed qualified digital signatures from a trusted eIDAS provider, issued for the EDPS's high- and mid-level management.

eIDAS is an EU regulation with the purpose of governing electronic identification and trust services for electronic transactions, allowing for secure and seamless electronic interactions using safe forms of electronic identification scheme.

As such, these digital signatures fill a gap that had been previously identified and provide the highest level of integrity, authentication and non-repudiation to the documents in digital format signed by the EDPS.

6.3.

Systems Oversight and Technology Audits

T&P's sector specialised in overseeing systems and technology audits is growing, taking care of audits of large-scale IT systems, and managing personal data breaches, as well as other initiatives detailed below.

6.3.1.

Audits

In 2023, two technical audits were performed: one on the Internal Market Information System (IMI) managed by the European Commission's DG GROW, and one on the Schengen Information System (SIS) managed by eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems.

Audits allow us to check whether EUIs that operate IT systems, especially large IT systems, have put in place the necessary technical measures to comply with EU data protection law and protect individuals' personal data.

Data Protection practices in DG GROW

In our audit, we were inspecting DG GROW's Internal Market Information System (IMI), which is a secure, multilingual, online tool that facilitates the exchange of information between public authorities involved in the practical application of EU law.

Our onsite inspection focused on the verification of the performance of some data protection measures according to the [IMI Regulation](#) and Regulation (EU) 2018/1725. We also delved into, amongst others, some of the IT's security aspects taking as reference the ISO Standard 27002:2022, which is an international standard for IT and information security.

Following our audit, a final report including recommendations was addressed to DG GROW that we will follow up on in 2024.



Schengen Information System audit

As for the Schengen Information System, we are under legal obligation to carry out an audit of the processing of personal data by eu-LISA according to international auditing standards at least every four years.

Usually, a report on these type of audits is sent to the European Parliament, the Council, the Commission and to the supervisory authorities.

This year, the audit focused on information security, including security policies and management, risk mitigation, testing procedures, technical vulnerabilities, system specific legal requirements (access control management, logging and retention of logs, security incidents, specific rules for biometric data in SIS), and personal data breaches. We developed and applied a new approach to security audits following the international standard ISO27002. Several findings have been observed during the fieldwork. The final audit report is expected in 2024.

6.3.2.

Supporting the EDPB: website and mobile app audits

We continued to provide technical support to the EDPB in the auditing of websites, by equipping them with the expertise gathered in developing, our website auditing tool, the Website Evidence Collector (WEC), initially launched in 2019 and regularly updated since then. The WEC has provided the bases for a new EDPB own website auditing tool.

Similarly, we shared with the EDPB technical documents to help them set up a mobile app audit lab: an infrastructure to carry out mobile app audits with the aim to ensure consistent auditing practices across the EU.

As an added layer of support, we volunteered to moderate an EDPB expert group that meets a few times every year during which representatives of data protection authorities of the EU/EEA exchange views and further discuss new approaches to the auditing of apps or app security in general. To enhance these actions on mobile and website audits, we also continued the organisation of a workshop to provide more in-depth training to data protection authorities' staff, to equip them with the necessary skills and tools in this area.



6.3.3.

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 EU institutions, offices, bodies and agencies (EUI) have a duty to report personal data breaches to the EDPS, unless a risk to the affected individuals is unlikely. Every EUI 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 concerned must also inform the concerned individuals without unnecessary delay. These obligations apply also for breaches on operational personal data.

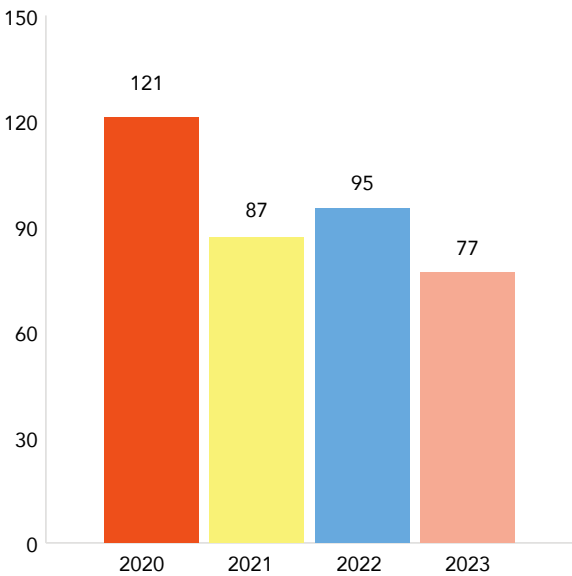
Chapter 9 of Regulation (EU) 2018/1725 introduces the data breach notification requirements for operational personal data, additional requirements for notifying competent national authorities may be introduced in the specific EUIs' Regulations (e.g. Europol and Eurojust). For the European Public Prosecutor's Office, similar notification requirements are introduced by Regulation (EU) 2017/1939.

In 2023, the EDPS has integrated strategically additional human resources for the management of the incoming personal data breach notifications and the development of efficient supervisory mechanisms. It is our goal for the years to come to develop further this area of managing personal data breaches, by providing EUIs with valuable technical advice to help them tackle personal data breaches, supporting more efficiently individuals and to proactively develop measures to avoid future incidents.

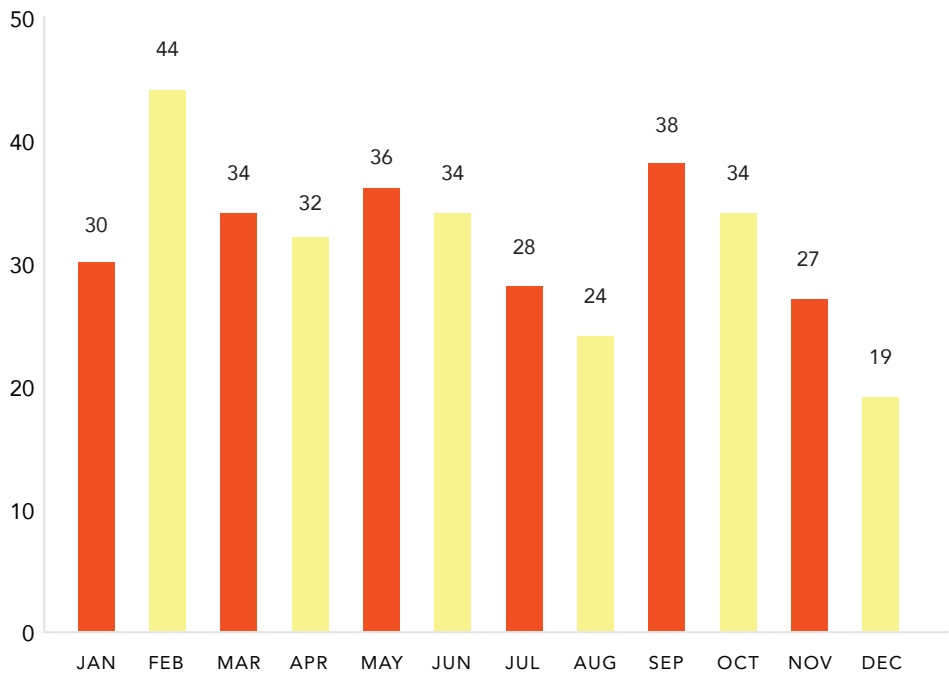


Number of personal data breaches notification in 2023

In 2023, we received and assessed 77 new admissible personal data breach notifications under Regulation (EU) 2018/1725. Overall, there was nearly a 19% decrease compared to 2022, during which we received 95 personal data breaches.



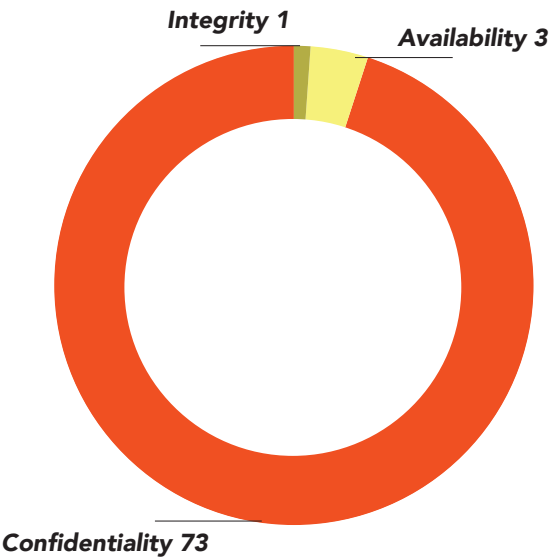
Number of Personal Data Breach Notifications for the years 2020 - 2023



Number of Personal Data Breach Notifications per month for the years 2020 - 2023

Type of personal data breaches in 2023

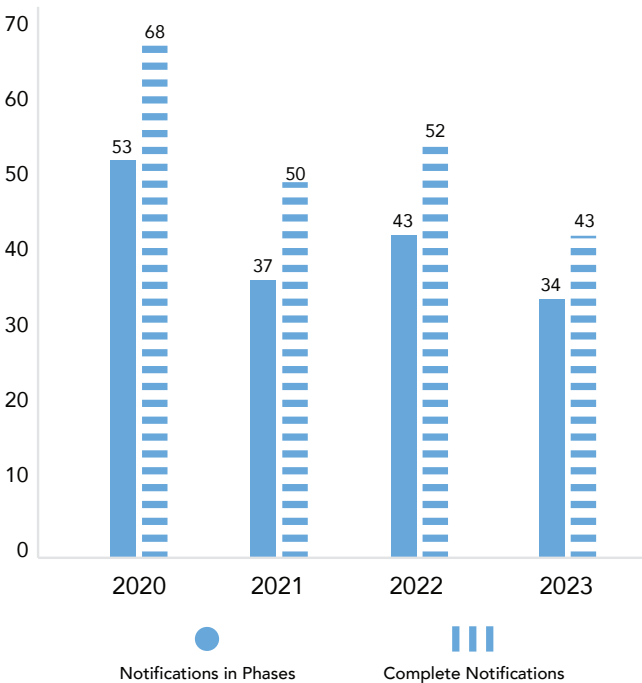
A personal data breach may be due to a confidentiality, availability or integrity breach or a combination of the above. During 2023, 73 cases posed primarily a breach of confidentiality. 1 case covered an integrity breach and 3 cases included availability breaches. Amounting to 77 submitted data breach notifications, 5 cases presented a combination of all types of breach.



Type of Personal Data Breaches in 2023

Type of Data Breach Notification - Category complete/in phases (2020-2023)

In 2023, the EDPS received 43 comprehensive personal data breach notifications and 34 notifications in phases. By the end of 2023, not all notifications in phases had been yet finalised from the relevant EUIs. As shown below, during the 2020 - 2023 the proportion of comprehensive notifications and notifications in phases did not differ significantly in comparison to the previous years.

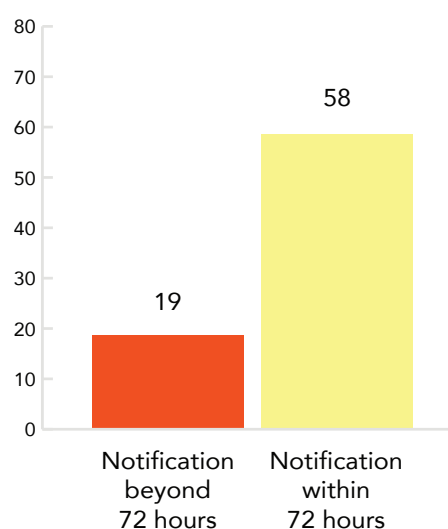


Type of Notification for the years 2020 - 2023

Notification within the 72h

Concerning the notification of personal data breaches within 72 hours, 58 notifications were submitted within 72 hours, whilst 19 notifications were delayed by the controllers due to various reasons. With regard to the 19 delayed notifications, in some cases, the delay was due to the controller trying to identify how individuals' personal data was 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 situation, we always advise EULs to review and simplify their internal processes for personal data breach notifications in order to meet the legal deadline and comply with the accountability principle.

In comparison to last year, the number of cases beyond the 72 hours significantly decreased. We interpret this as an improvement for all reporting EULs in managing internally the occurred data breaches.



EDPS - Number of DB Notification within 72 hours in 2023

Root cause of Personal data breaches

Examining this year's root causes of personal data breaches, human error remains the most common one, despite the observed drop in the number of submitted data breach notifications.

With cases where human error is the root cause, the usual pattern includes sending an email with confidential information to the wrong recipients or putting all recipients in carbon copy (cc) instead of blind carbon copy (bcc), whereas their contact details were not to be disclosed to the rest of the recipients list.

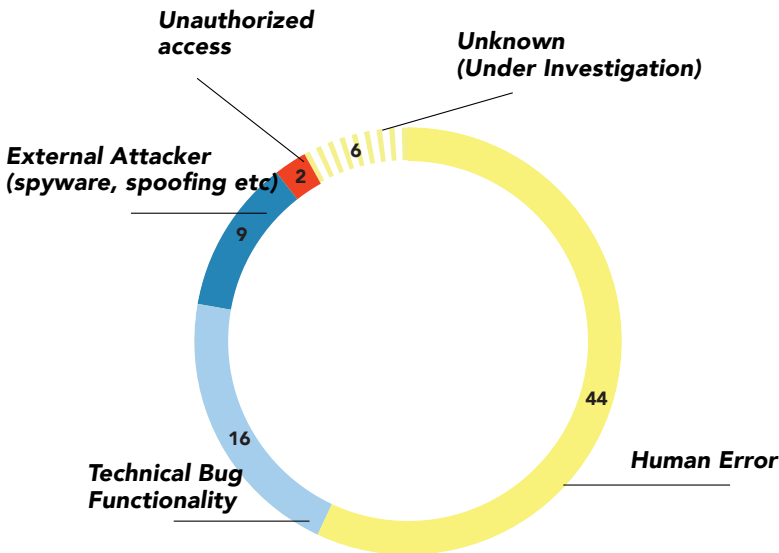
Following the same pattern, we have also received personal data breach notifications concerning the publishing of documents without removing personal data in the context of EULs' access to document requests and transparency procedures. Similar to previous years, we have observed a high number of human errors during recruitment processes. In some cases, results occur during selection processes during which information was sent to the wrong candidates. Furthermore, a high number of notifications involving personal data breaches, such as sending the wrong medical invoices to wrong recipients.

Contrary to 2022, personal data breaches caused by technical errors rank second place on the root cause podium. The most usual type of technical errors results in erroneous access authorisations often accidentally triggered during a software tool update.

Lastly, despite the low figure of 9 declared cases, external attacks count as the third most common root cause of personal data breaches this year.

In many cases, these attacks were due to the insufficient implementation of security measures and procedures by EUIs, related to a lack of secure design, secure coding and patching of systems. The absence of data protection by design was highlighted in such cases, since the data breaches could have been avoided if effective security measures and in particular data retention periods had been deployed in appropriate manner as to minimise the attack surface.

In 2022, we had 22 cases caused by external attacks. In 2023, we observed a decrease of 59%. This is unexpected and raises the following question: is it possible that so many EUIs did not suffer any personal data breach or is there another reasonable explanation behind this phenomenon? At the same time, the number of cybersecurity incidents within the EU are on the rise and they affect greatly the processing of personal data. There might be different reasons explaining these results: DPOs are not alerted, data breach risk assessment conclusions are on the optimistic side or EUIs are not aware of being under attack.

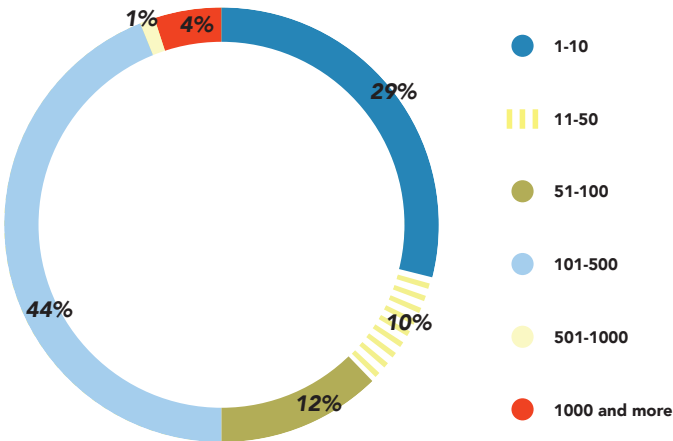


Root cause of Personal Data Breach Notifications in 2023

Number of affected individuals of Personal Data Breaches

In the majority of cases - 44% approximately - 101 to 500 data subjects were affected. A small number of individuals - between 1-10 - were affected in 29% of cases. 12% of the cases concern group of individuals between 51-100 data subjects.

In 3 cases of personal data breaches, which equals to 4% of the total cases, more than 1000 individuals were affected.



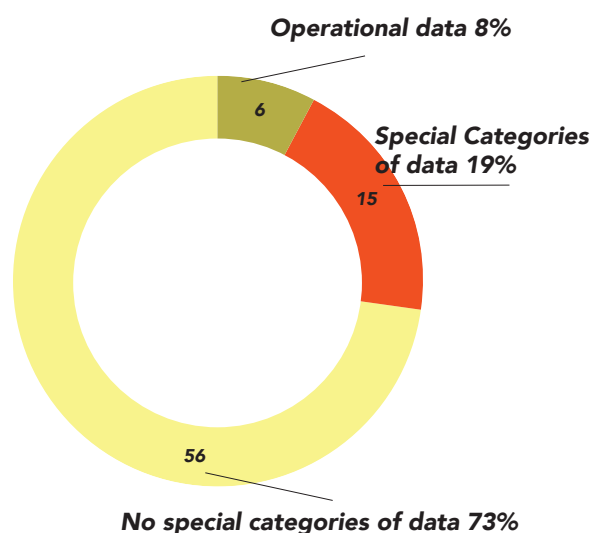
Number of affected individuals per DBN in 2023

Categories of data - Personal Data Breaches in 2023

19% of the personal data breach notifications received this year involved [special categories of data](#). In the majority of cases, health data is concerned, mostly associated with errors when sending medical invoices, especially during the reimbursement processes.

In those areas, we recommend that EUIs raise their staff's (or contractors) awareness, and consider additional safeguards to avoid human error.

In 8% of the personal data breach cases, the confidentiality of operational data was affected. The categories of individuals involved included suspects and individuals under investigations, as well as information related to officers being assigned specific tasks. Concerning the operational data breach notifications we received, no special categories of data were affected.

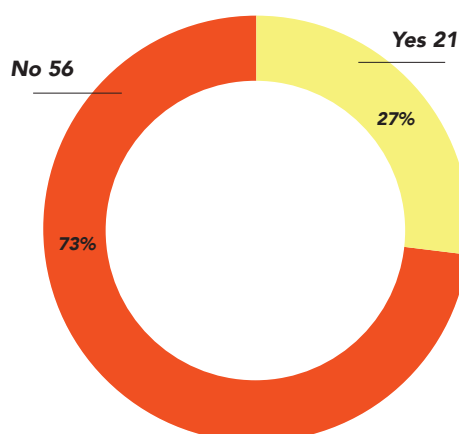


Categories of personal data in Data breach notifications in 2023

Notification to the Data Subject - Personal Data Breaches

In 21 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 of being transparent and may even propose this option to EUIs, when there is a sensitive context to the data breach. In 2023, there was 1 case in which we assessed that the occurred breach was of high risk, which was in contradiction with the EUI's initial assessment, and we therefore asked them to notify the affected individuals.

It needs to be noted that during the further analysis of those personal data breaches that were notified in phases, the assessment of the risk and thus of the requirement for controllers to notify data subjects may change following their conclusive analysis.



Notification to data subjects in 2023

Other data breach notifications

We also received notifications outside EDPS's competence. In 2023, the EDPS received four personal data breach cases from EUIs for which there was no obligation to notify. In these cases, we assessed that it was unlikely that there was a risk posed to individuals and therefore informed EUIs to just document the breach in their internal register.

We also received 9 notifications sent from private companies or individuals (whistle-blowers), which were outside the scope of Regulation (EU) 1725/2018.

6.3.4.

Website Evidence Collector

In 2023, the EDPS released a new version of the Website Evidence Collector (WEC). The WEC collects evidence of personal data processing, such as cookies and similar tracking technologies.

Whilst we use this tool to carry out our own website audits and investigations as a matter of accountability, the WEC is also available for public use. Indeed, this setup allows website controllers, data protection officers and users to better understand what information is transferred and stored during a visit of a website. With the WEC, owners and data controllers are able to self-assess their websites' compliance and foster accountability. Consumers and NGOs can also use the WEC to check if websites comply with the regulatory framework.

The WEC source code is available on the EU's JoinUp platform and on GitHub under the European Union Public Licence (EUPL v1.2). The tool is also available to download on Windows, Mac and Linux computers.

6.4.

Providing our expertise to other EDPS Units

With its expertise in analysing technological developments and their impact on privacy, T&P has contributed to other EDPS Units' work, especially in the area of policy making, including on the EDPS-EDPB Joint Opinion on the Digital Euro and the EDPS Opinion on the Proposal for Artificial Intelligence Act, as well as in the EDPS' enforcement activities by participating in audits of European Centre for Disease Control (ECDC), Europol and Eurojust, for example.

Likewise, T&P cooperated with other data protection authorities and other regulatory or administrative authorities in the development of common assessments and recommendations on emerging technologies.

Additionally, T&P provides guidance to EUIs on the safeguards needed to ensure data protection when using specific technologies. As such, T&P also informs and advises data controllers about their rights and responsibilities in the field of IT and information security. The Unit also monitors the state of play of information security across all technological fields to help ensure that data controllers properly put in place their security obligations.

As the EDPS continues to expand its activities in the field of technology monitoring, especially related to Artificial Intelligence, the T&P unit continues to engage with external stakeholders, such as civil society, academia and industry.

6.5.

Cooperation with other Institutions

With the goal to enhance a coherent and consistent application of data protection, and upholding individuals' privacy, the EDPS cooperates with other EU institutions.

Pairing up Privacy and Cybersecurity

The EDPS further collaborated with ENISA, the EU's Cybersecurity Agency, after formalising its strategic cooperation with a Memorandum of Understanding signed in November 2022.

Both organisations work together on designing, developing and delivering capacity building, awareness-raising activities, as well as cooperating on policy related matters on topics of common interest, and contributing to similar activities organised by other EU institutions, bodies, offices and agencies (EUIs).

Aside from our collaboration with ENISA, we regularly conduct trainings with the EDPS' staff and EUIs' staff to enhance cybersecurity awareness and their ability to prevent and avoid cybersecurity incidents, especially in light of the upcoming enforcement of the new Cybersecurity Regulation for EUIs.

Aside from this collaboration, the EDPS actively participated in the Annual Privacy Forum 2023 to discuss the latest developments in AI and its impact on privacy and data protection, with a focus on the role that data protection authorities can take in the regulating and enforcing of AI.

JASPER exercise

The EDPS took part in an annual cyber-exercise for EUIs, co-organised by ENISA and CERT-EU, the Computer Emergency Response Team for the EU institutions, bodies and agencies.

In this context, the EDPS informed participants - composed of EUIs' members of staff - on how to manage security incidents, highlighting that a cybersecurity incident may also be a personal data breach. In our presentation, we highlighted that EUIs need to setup internal personal data breach management processes to comply with the legal requirements of Article 34 & 35 of Regulation (EU) 2018/1725 on personal data breaches.

CHAPTER SEVEN

Communicating on data protection



As an organisation, we strive to be transparent - **explaining in clear language, accessible to all, what we are doing and why.**

To this end, over the years we have developed, and cemented, a strong online presence, primarily through our social media channels, and the EDPS 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.

7.1.

The EDPS' online presence

With the aim of diversifying our online presence, we have built, and continue to expand, a strong online presence, on our traditional social media channels, as well as on our new alternative social media channels, EU Voice and EU Video, 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

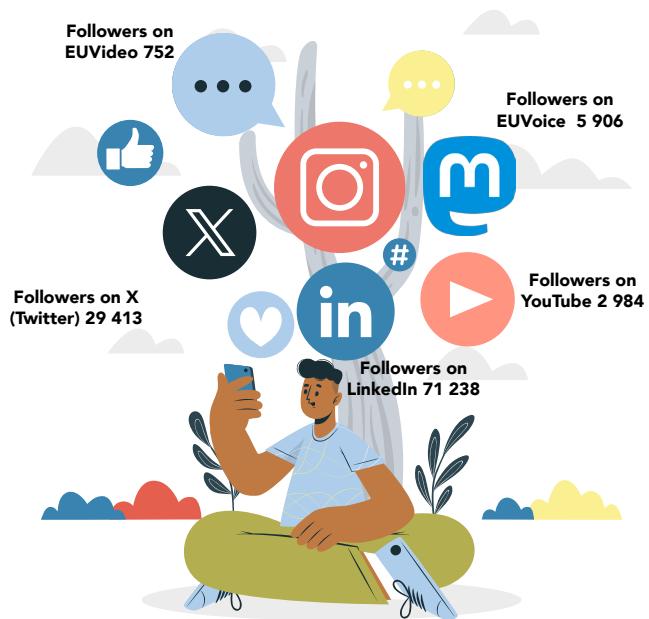
In this highly digitised world, social media has become one of the most common communication tools. Over the years, we have built a well-established presence on three social media channels, namely X (formerly known as Twitter), LinkedIn and YouTube, which we use to reach a global audience easily and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



7.1.2.

Cementing our presence on EU Voice and EU Video

With the aim of seeking alternative communication tools that promote a more democratic, decentralised and privacy-friendly model of social media, we multiplied our presence on our social media platforms: **EU Voice and EU Video based on free and open source Mastodon and Peertube software**, launched in February 2022 to serve as additional communication channels to our X and LinkedIn accounts.

On **EU Voice**, we publish short posts about our work, such as our Opinions, latest press releases, and consultations, which our followers can comment on to interact with us and other users, bookmark a publication, share with others, and more.

On **EU Video**, we publish short informational videos on our activities, podcast episodes, as well as video recordings of some of our past events.

We presented the project, our findings and best practices in a panel called “Digital tools and open data enhancing civic engagement” at Europcom organised by the Committee of the Regions (CoR).

7.1.3.

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.

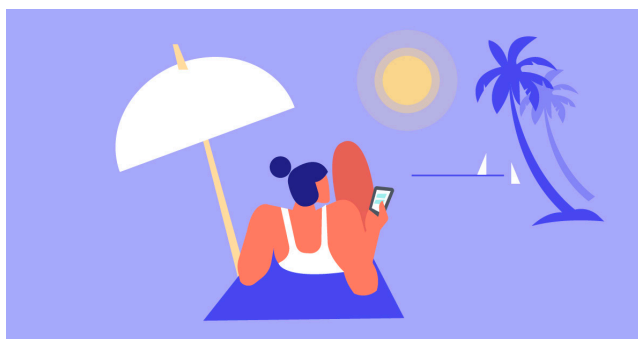


#InCaseYouMissedIt: As we continue to welcome new followers to our ever-growing social media community, we run the #InCaseYouMissedIt campaign on our social media accounts to raise awareness of less high-profile topics and to remind our audience about activities that they might have missed over the past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



European Cybersecurity Month: In October 2023, we celebrated European Cybersecurity Month. To mark the occasion we prepared an extensive social media campaign to raise awareness on social engineering techniques used in cyberattacks, including a comic on pretexting.

#StaySafe: Observing an increase in the number of incidents related to privacy and data protection in summer, we organised a mini-series of short animated videos of tips for our target audience to protect their personal data when on holiday.



This year, our socials media channels were essential tools to amplify the EDPS' strategy on Artificial Intelligence, its landmark event on the privacy implications of the proposed Child Sexual Abuse Material Regulation, as well as our employer branding outreach activity - Espresso with #teamEDPS, to name a few examples.

7.1.4.

The 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. For example, we completed the migration of our website to Drupal 10. We have added new filters to facilitate the search of different publication categories. We introduced the eTranslation widget to obtain quick raw machine translations of a text into any official EU language.

7.2.

Bringing our work one step closer

Data Protection is a topic that has gained a lot of attention, especially since the General Data Protection Regulation has been enforced. Individuals are more aware of their rights, and the value of their personal data, even more so since COVID-19.

As a result, our work has attracted new audience, both experts and non-experts in data protection. To match this new interest, we have continued to deliver the **EDPS Newsletter**, providing frequent and short updates on our activities.

Complementing this, we have developed, and launched at the end of 2022, a new EDPS Podcast Series, the **EDPS Newsletter Digest**, as well as the expansion and creation of other series, branching out in terms of medium and attracting a new audience.

We continued to deliver a more personal outlook on data protection with our **EDPS Blog**, where the EDPS Supervisor, Secretary-General and some Heads of Units share their reflections on data protection.

7.2.1.

Monthly updates: the 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 2023, 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.

One year of podcasting: the Newsletter Digest

In December 2022, we started a new podcast series, 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 selection of updates on our latest work in the fields of Supervision & Enforcement, Policy & Consultation, Technology & Privacy. 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.

Now active for a year, and with 10 episodes published, the Newsletter Digest Podcast has evolved, with bonus episodes including exclusive interviews with actors in the data protection field.

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. From interviews with thought-provoking experts, to deep dives into current events, our goal is to provide information on EDPS' work and to explore the EU data protection and privacy framework.



7.2.3.

Our blog: a more personal outlook on data protection

Now active for over seven years, the EDPS blog 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 2023, we published 8 blogposts on an array of subject matters. This medium has proved to be useful, not just in 2023, but also in recent years, to provide more details on:

- what is discussed during the bi-annual meetings of the network of DPOs;
- our technological monitoring efforts;
- the events that we have organised;
- an insight into the EDPS-EDPB traineeship.

7.3.

An interactive perspective on data protection

Diversifying the way we communicate and how to ensure engagement with the topic of data protection and what we do as an organisation is one of our core goals. One effective way we do this is through the publication of **Factsheets** and **Infographics**: a one-page document breaking down a key concept of data protection in a clear, concise, and visually pleasing way.

Adopting this communication style was particularly effective this year when explaining the EDPS' work in the field of Artificial Intelligence, or explaining how the EDPS conducts investigations.

7.4.

Public Relations

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

7.4.1.

Press Releases

This year we issued 13 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:

- the EU's financial package, including the digital euro and finance and payment services;
- the Artificial Intelligence Act;
- our enforcement actions;
- personal data and public safety.



Press Releases: 13

7.4.2.

Media interest

The topics that garnered the most attention in 2023 are detailed below, and include our enforcement actions, such as our investigations, audit reports, and orders.

We also receive press and media requests about our role in the legislative process, mainly about artificial intelligence, technological developments, digital currencies, child sexual abuse material, health data space, for example.

7.4.3.

Public requests

In 2023, 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.



7.5.

Events

2023 was marked by a multitude of events. The appetite of our community to engage in pivotal and current data protection issues continues to grow.

The I&C Unit supports the EDPS in its mission to interact with various actors, including data protection and technology experts, EU and national legislators, to help advance the global standards of data protection.

This year we organised 10 events that followed different formats, including conferences, seminars, workshops; and we actively supported the organisation of 4 other major events. With these efforts, we reached an audience of more than 20 000 people across all events.

7.5.1.

Celebrating the 5th Anniversary of the GDPR

To mark the 5th anniversary of the entry into application of the General Data Protection Regulation, we co-organised with the German Federal Commissioner for Data Protection and Freedom of Information, and the Bavarian Data Protection Commissioner the high-level event: "5th Anniversary of the GDPR: Still a benchmark in the EU digital landscape?"



The event, taking place on 23 May, brought together 400 stakeholders to reflect on the impact of the GDPR and on the new challenges that emerged after 5 years of its application.

7.5.2.

EDPS opens its Strasbourg Office

One of the EDPS' highlights of the year 2023 was the opening of its Office in the European Parliament of Strasbourg.

With this new office in the European Parliament in Strasbourg, the EDPS aims to provide additional support in the EP legislative process - including during the plenary sessions - fulfilling its role as advisor to the EU legislators. With data protection becoming increasingly engrained in EU legislation, the new EDPS office in Strasbourg provides an opportunity for closer cooperation and engagement with policymakers. The objective is also to reinforce the cooperation with other EU institutions present in Strasbourg - the European Ombudsman, the European Court of Human Rights and the Council of Europe.



7.5.3.

Workshops and Seminars

Artificial Intelligence

With the growing interest and developments in artificial intelligence (AI), the I&C Unit supported the EDPS and the EDPB trainees in the organisation of a workshop on the impact of this technology on data protection. At the event, discussion will focus on the balance between the benefits that Artificial Intelligence can bring to society and the risks that it may pose to individuals.

International Organisations Workshop

We continued to contribute to the organisation of the International Organisations Workshop, a concept launched in 2005 that aims to bring together International Organisations to share experiences and best practices in the field of privacy and data protection. Each workshop is co-organised by the EDPS and a different International Organisation for each edition.



On 23 and 24 October, the EDPS also co-hosted with INTERPOL the 2023 edition of the International Organisations Workshop on Data Protection (IOW). Participants discuss the most recent regulatory developments at international level and analyse their implications for International Organisations.

Seminar on combatting Child Sexual Abuse Material

In light of regulatory developments on the topic of Child Sexual Abuse Material, we hosted and organised a EDPS Seminar on the CSAM proposal: “The Point of No Return?” on this matter on 23 October 2023, to provide a platform for stakeholders who have been warning about the risks associated to the legislative proposal. In particular, the workshop addressed how the CSAM proposal would fundamentally change the internet and digital communication as we know it.

Seminar on the fundamental rights to privacy and data protection

The seminar we hosted on the essence of the fundamental rights to privacy and data protection on 8 November 2023 aimed to provide an opportunity for meaningful exchanges amongst data protection experts on the meaning of the ‘essence’ requirement of the right to the protection of personal data as fundamental right.

Europe Day

Every year in May, we celebrate Europe Day, marking the anniversary of the Schuman Declaration that brought peace and unity to Europe.

Being fully engaged in this celebration year upon year, we joined, together with the European Data Protection Board, the European Commission's Open Day at the Berlaymont Building. For an impactful presentation of our institution, we prepared an exhibition stand full of interactive activities - suitable to all ages - to explain what we do and why.

This Europe Day was also special for the EDPS because it was the first time our institution participated in the EU Open Day of the European Parliament in Strasbourg, providing us with the opportunity to meet a wider and diverse group of EU citizens.

An increase in Study Visits, a rising interest in our work

With 12 study visits carried out in 2023 gathering 306 participants, we increased the number of Study Visits organised in 2022.

Study visits are an essential part of our communication strategy and an essential way for us to connect with our stakeholders specialised in privacy and data protection. 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.

This format allows us to meet and discuss about everyday data protection matters, and share first-hand knowledge, perspective, culture and values.

Meeting small groups also allows us to have more in-depth conversation tailored to visitors' interests and studies.

On top of these study visits, we also hosted in our premises a Leadership Circle of high-level managers of EU institutions, bodies, and agencies to discuss the impact of AI on our organisations, providing a particular spotlight on the risks to the fundamental rights of privacy and data protection. We hosted this Leadership Circle at the request of the European School of Administration (EUSA).

7.6.

The EDPS Employer Branding

Since 2021, we have been executing our Employer Branding Strategy 2021-2024, which includes a variety of communication activities, to increase the EDPS' visibility and strengthen its image as an attractive career destination.

One of the ways we are delivering this strategy is by creating the EDPS Staff Ambassadors Club who share their experience of working at the EDPS. With their help, we have rolled out this year a LinkedIn campaign known as #teamEDPS presenting testimonials of the EDPS Staff Ambassadors and aiming at promoting the EDPS as a workplace.

In 2023, we delivered a communication campaign with a series of short videos, titled "Espresso with #teamEDPS" in which our staff ambassadors gave an insight into their work and career paths whilst drinking coffee or tea.

7.7.

Collaborative Communication

We have continued our close cooperation with other EU institutions ('EUIs'), bodies, offices and agencies 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.

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. 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.

7.8.

Planning ahead for 2024: the EDPS' 20th anniversary

From September 2023 onwards, we have dedicated much creativity and resources in preparing the EDPS' 20th anniversary.

Looking back on two decades of safeguarding citizens' privacy and data protection rights, we are organising 4 key initiatives to reflect together on the current areas of improvement and future challenges in the data protection landscape.



For this landmark event, we are developing, planning and creating:

- a [dedicated website](#) featuring all of our activities as well as a historic timeline;
- a forward-looking book on data protection;
- a Summit scheduled in June 2024;
- the publication of 20 initiatives illustrating the EDPS' continuous aspiration to lead as a modern data protection authority; and
- the production of 20 talks gathering experts from all around the world to discuss privacy.

CHAPTER EIGHT

Human Resources Budget 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.

8.1.

Reshaping the EDPS to tackle data protection challenges

Identifying the need for our organisation to evolve to match our goals and vision, HRBA carried out a number of activities to mirror the EDPS' expansion.

8.1.1.

New Units and specialised Sectors

The EDPS appointed its first Secretary-General in July 2023 to provide strategic advice to the Supervisor and to oversee the institution's activities, and its effective functioning. With this role, the Secretary-General also supports the Supervisor in engaging with stakeholders and other actors in the field of data protection.

Fully reflecting the organisation's priorities and keeping up with the rapidly changing digital regulatory landscape, the HRBA Unit was instrumental in the transition and creation of specialised units and sectors at the EDPS.

Addressing the development of new technologies, together with its risks and opportunities, three sectors were also created in the Technology and Privacy Unit. One for the oversight and auditing of IT systems, another to anticipate new technologies and their impact on privacy and data protection, and a sector to develop the independent digital transformation of the institution.

HRBA also accompanied the transition of two Sectors into Units: the Governance and Internal Compliance Unit to ensure the institution's own accountability and the Information and Communication Unit to publicise the EDPS' activities, in April 2023.

To embrace the EDPS' growth over the years, the HRBA Unit put in place this year a series of activities to bring together Heads of Units, fostering a team spirit amongst managers.



8.1.2.

Adapting working conditions

As a forward-looking institution, the EDPS has decided to pursue its hybrid-working regime first piloted in May 2022. This was proved successful according to a pulse survey carried out amongst EDPS and EDPB staff in April 2023.

8.1.3.

Automating procedures

We pursued our efforts in further modernising and simplifying some human resources and administrative processes by automating certain of our activities, such as putting in place the CCP module (leave on personal grounds module) to manage staff's requests for career breaks, when eligible, via Sysper, an HR management tool. In the same vein, we also reviewed our selection procedure process with a view of simplifying the evaluation report template.

8.2.

The EDPS as an employer

Equipping our employees with the appropriate skills to work has a direct impact on our organisation's success. Reflecting this, we have continued to organise training sessions, job-shadowing programmes, and other initiatives.

8.2.1.

Staff satisfaction survey

Following the EDPS' Staff Satisfaction Survey, orchestrated by HRBA in 2022, to gain an understanding of the institution's working environment, a working group was established to analyse its findings.

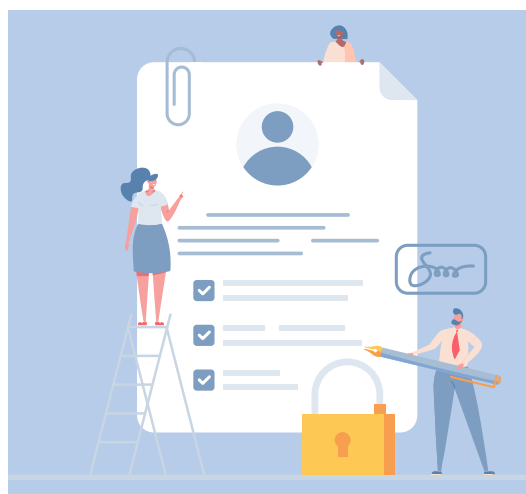
In April 2023, the working group presented a comprehensive report with 59 recommendations and actions, subsequently analysed by the EDPS' senior management, to decide on follow-up measures to take, to continue to foster a strong and positive working culture.

8.2.2.

Recruitment

We strive to bring together a diverse team of legal and technical experts, as well as other specialists in their field from all across the European Union, working to shape the world of data protection and our organisation.

This multifaceted background and different perspectives brought to the table allow us to respond creatively to data protection challenges and to find solutions that benefit society as a whole, especially the most vulnerable.



The HRBA Unit recruits staff for the European Data Protection Supervisor and the European Data Protection Board to ensure that the right people are selected to defend the fundamental rights to privacy and to the protection of personal data in the EUIs as they face new challenges, such as Artificial Intelligence.

Whilst the EDPS and the EDPB are composed of data protection experts, various other profiles to support the institution's increased workload are hired.

Against this background, and factoring in the turnover of staff to replace both in the short and long term, the HRBA Unit organised the selection and recruitment of 20 officials, 3 temporary agents, and 15 contract agents with different contract durations. Alongside managing the selection and recruitment procedures of new staff, the HRBA sector also oversees the monitoring and renewal of contracts for contract agents, temporary agents, and external providers throughout the year. Additionally, HRBA initiates the procurement procedure for the selecting and hiring of interim staff.

8.2.3.

Our traineeship programme



With our traineeship programme, we welcome 10 Blue Book trainees to the EDPS and the EDPB twice a year - once in October and once in March.

Any European citizen can apply to the programme, carried out as part of our Service Level Agreement signed with the European Commission. The programme allows young European graduates to better understand the work of the EDPS and EDPB. This experience benefits all parties involved: Blue Book trainees contribute substantially to the institution's activities, and, in turn, the EDPS and EDPB attract new talent with different perspectives, adding value to our work, building a dynamic working environment.

Proving the programme's success, there is a rising interest and demand in Units and Sectors from the EDPS and EDPB for trainees. In response to this trend, the HRBA Unit introduced in 2023 a rotation system to allow each Unit or Sector to benefit from one of the 10 trainees allocated at regular intervals. Additionally, the HRBA Unit coordinates the logistical arrangements of trainees to ensure their smooth and seamless welcome. In exceptional circumstances, and to respond to specific needs, the EDPS welcomed "atypical" trainees from other Data Protection Agencies. This opportunity was beneficial both for the institution and for the trainees.

8.2.4.

A new onboarding procedure

With the aim to foster a cross-collaborative culture, the HRBA Unit piloted a new onboarding procedure with informative sessions highlighting how each Unit works.

This new onboarding procedure was split into two half-day sessions.

The first onboarding session was opened by the HRBA Unit to explain the tools that the EDPS staff needs in their day-to-day tasks, followed by the Ethics Officer's presentation and respective presentations of the Policy and Consultation, Supervision and Enforcement, and the Technology and Privacy Units, as well as the EDPB.



The second session included a training on Human Resources' matters, such as learning and development, anti-harassment policy awareness, and diversity and inclusion, as well as on the institution's procurement procedures, the use of MIPS+ to record missions. Our information security, and data protection processes were also covered. The Staff Committee, acting as an independent support system for colleagues, also presented itself.

If successful, an extension of this procedure will be considered.

8.3.

Professional development of our staff

Focusing on the professional development of our staff to guarantee the longevity of the EDPS, we have continued to build a series of opportunities and carried out a plethora of actions, including investing in our job-shadowing programme, coaching, learning and development and more, to encourage staff to add new skills to their portfolio.

8.3.1.

Job Shadowing

EDPS and EDPB staff have benefited from a new inter-institutional Job Shadowing Programme, launched in June 2023.

The programme consists of a short-term exchange in which an EDPS or EDPB member of staff is paired up with a staff member of another EU institution, body, office or agency, to increase respective understanding and awareness of their work, role and tasks.

8.3.2.

Coaching

In 2023, we continued to provide internal coaching and other activities to EDPS and EDPB staff to help improve individual job performance and relationships at work.

Coaching focuses on developing strengths, making changes and helping find specific solutions to professional challenges.

Our internal coach conducted over 12 individual sessions in full confidentiality in 2023. On top of this, coaching was provided to many Units and Sectors of the EDPS. The aim of these sessions is to accompany Units and Sectors in improving their working relationships, defining the mission and identity of their Units or Sectors and setting priorities and goals for their work.

Throughout 2023, the management team of the EDPS also benefited from a one-year team-coaching path, co-facilitated with a designer for leadership development from the EU's school of administration (EuSA).

The objective of the team coaching were two-fold: to create space for the management team to meet together in more informal settings, to discuss strategic issues in particular, and to help them connect on a personal level in a way that could benefit regular professional interactions. The team-coaching path will conclude in early January 2024 with a management team seminar in the house of Jean Monnet, France.

Additionally, we pursued our co-development programme, a group coaching in which participants learn from each other and consolidate their professional practice. This co-development programme involving 6 sessions was organised in 2023 for Heads of Sectors and Activity, as well as Deputy Heads of Units of the EDPS.



8.3.3.

EDPS Away Day

In September 2023, an EDPS Away Day was organised for all staff, with a special focus on the EDPS' history, recognising colleagues' contributions to the creation of the institution and in preparation for the 20th Anniversary that will be celebrated throughout 2024.

The Away Day, championed by the HRBA Unit, was met with enthusiasm and a high-level of engagement from over 100 participants.

8.3.4.

Learning and Development

A new Learning & Development (L&D) strategy was adopted in June 2023 to replace the outdated strategy dating back from 2013.

The new strategy sets a comprehensive frame around L&D, defines the role of HRBA, managers and staff members and echoes with the new ways of working and learning.

8.4.

Managing our resources to meet expectations

Monitoring, planning, reviewing and executing our budget allows us to meet the organisation's objectives, in alignment with the EDPS Strategy 2020 - 2024.

The HRBA Unit also deals with administrative matters, such as ensuring that newly recruited staff have all the necessary equipment to work, as well as the necessary accesses to IT accounts and other facilities and also follows up on matters relating to our headquarters rented from the European Parliament.

8.4.1.

The ins and outs of our budget

Budget execution

The 2023 EDPS operating budget amounted to EUR 22,711,559.

Compared to the 2022 final budget, the operating budget increased by 12%.

In terms of budget execution, the commitment appropriations show an implementation rate of 96%.

This positive trend was made possible due to an accurate monitoring of the budget forecast and sound planning of the EDPS' activities, including events and conferences.

Budget preparation

Although very challenging in view of the annual inflation and unexpected high costs of living, the 2024 budget exercise was conducted successfully to meet the EDPS' planned priorities.

As was the case for previous budget exercises, the need to follow a rigorous approach regarding administrative expenditure and staffing of the European institutions, bodies, offices and agencies (EUIs) in general has remained an imperative element in the preparation of the 2024 Draft Budget.



In the EDPS' Draft Statement of Estimates for 2024, significant cuts were made by the European Commission and the Council, in line with the general saving needs imposed on most of EUIs.

Consequently, a rethinking of the priorities and reductions or even complete cuts of some of the initiatives foreseen for 2024 will be necessary. The final approved budget foresees an increase of expenditure of 7.12% compared to 2023.

Budget monitoring

2023 followed the implementation of the Bluebell budget software.

The EDPS uses Bluebell to establish and revise forecasts for the budget based on data uploaded and updated by operational Units.

Bluebell also allows us to give a refined view of all budget lines by detailing them into actions and linking these actions with posting criteria in ABAC, the financial software used in the European Commission and other EUIs, so that the forecast can be compared in real time with the actual execution.

Using this system has increased our efficiency in the preparation, monitoring and follow-up of budget execution. In addition, the tool proves to be useful for audit trail purposes and ex-post control as files and supporting documents are available anytime in the system.

8.5.

Finance

The number of payment transactions (1335) increased substantially in 2023 compared to 2022 (799): meaning an increase of 67%. This can be explained due to a high number of meetings and expert reimbursements.

8.6.

Public Procurement

In 2023, we launched numerous public procurement procedures, taking into account both the EDPS' and EDPB's working programmes and plans for the upcoming year. As per last year, this included the need for outsourcing certain activities, such as particular events, conferences, and other projects.

In this respect, part of the EDPS' HRBA Unit supported both institutions in these procedures, by ensuring that these are conducted in compliance with the budgetary principles laid down in the Financial Regulation.

More specifically, the Unit's focus is to make sure that the external contractors collaborating with the EDPS and the EDPB meet the necessary moral and ethical standards expected from all EUIs; uphold the highest professional conduct throughout the contract; and respect the environmental, social and human rights defended by the EU.

Throughout the entire process of a public procurement procedure, the HRBA Unit prioritises an open, fair, transparent selection and competition process. The aim is to make these procedures more accessible to a wider range of talents, irrespective of a contractor's background. Indeed, we believe that an environment favouring healthy competition fosters a qualitative collaboration between the EDPS and/or the EDPB and the contractor(s) in question.

This year, the EDPS continued to participate in large inter-institutional Framework Contracts, to achieve a higher degree of administrative efficiency. The main inter-institutional framework contracts used are related to IT consultancy, audio-video, interim services, office supplies and office furniture.

In addition to that, in 2023 we conducted two procedures for framework contracts for the EDPS' Legal Service and the Information and Communication Unit.

8.7.

Accounting

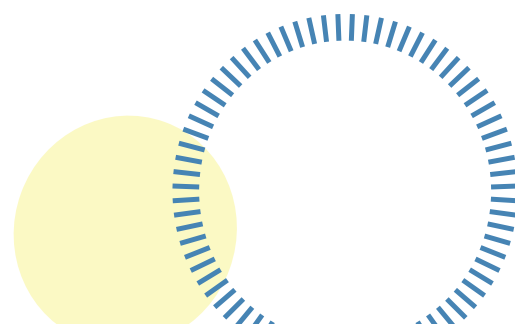
According to the legal framework of the financial regulations and established deadlines, as an organisation, we contribute to the preparation of the provisional annual accounts sent to the European Commission.

The scope of this procedure is to ensure that all expenses and revenues are included in the correct financial year and that the annual accounts are complete and represent fairly the financial position and budget implementation of the EDPS.

The annual accounts cover the period from 1 January to 31 December 2023 and comprise the financial statements and the reports on the implementation of the budget. These are prepared in accordance with the rules adopted by the accounting officer of the European Commission, which are based on internationally accepted accounting standards for the public sector.

Amongst other tasks required, we prepared the Accrual Calculation, the Preparation of the Cut-off file, the Fix Assets Reconciliation, the Intercompany Reconciliation and the Preparation of postings. The provisional annual accounts will have to be transmitted, by the 1 March, to the European Court of Auditors (ECA).

The final annual accounts are sent to the accounting officer of the Commission, the Court of Auditors, the European Parliament and the Council by 1 July. The ECA scrutinises the final annual accounts and includes any findings in the annual report for the European Parliament and the Council. The accounting exercise is extremely important as the discharge decision is also based on a review of the accounts and the annual report of the ECA.



8.8.

A new inventory management system

For the inventory of the EDPS' physical assets, including office equipment, furniture and IT devices, the HRBA Unit prepared and conducted the migration to ABAC Assets, an accounting system hosted by the European Commission.

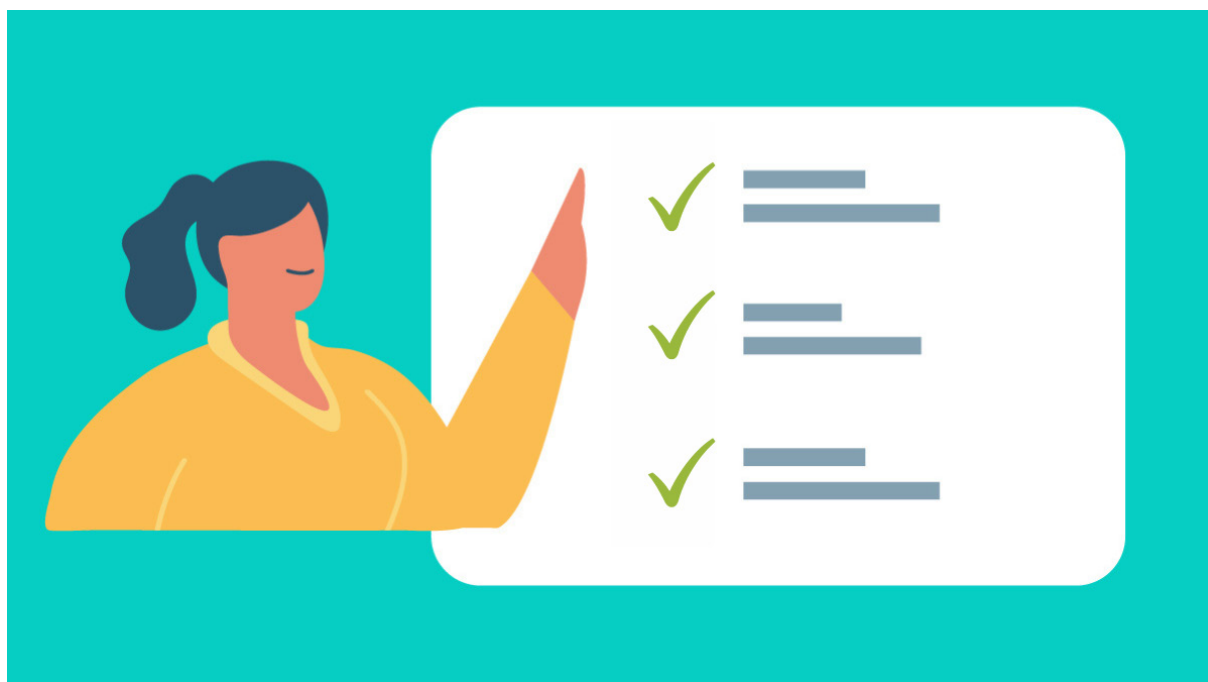
The migration was successfully completed in December 2022 and the new system now promises considerable efficiency to carry out future inventory stocktaking and yearly account closure exercises.

8.9.

Managing missions more efficiently

In November 2022, the EDPS joined a PMO pilot project for the management of missions in a shared mode, meaning that staff going on trips for work purposes can benefit directly from services offered by the PMO's mission experts; this is particularly relevant when it comes to declaring mission expenses and related reimbursements.

From July 2023, the EDPS starts using new and improved version of MIPS called MIPS+, the mission processing system. Two internal trainings were provided to EDPS and EDPB staff in order to use this new application effectively. In January 2023, in order to simplify and improve the missions management follow-up, the EDPS decided to put in place a mission budget envelope per Unit.



CHAPTER NINE

Governance and Internal Compliance



The Governance and Internal Compliance (G&IC) sector evolved into a unit in 2023, to enhance already-created synergies amongst institutional functions covering:

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

This organisational change acknowledged the Unit's important role and activities in supporting the EDPS' own accountability and compliance efforts.

Concerning **records and knowledge management activities** during the year, in 2023 the G&IC unit steered the completion of on boarding ARES (Advanced Records System) specifically for administrative activities by the end of October. As a result, the EDPS joined a growing number of EU institutions, bodies, agencies using this document management application. ARES operates in parallel to the EDPS Case Management System (CMS), the latter is designed for core business cases and documents. G&IC is managing and maintaining both applications.

Planning and internal control activities were carried out throughout the year: management of the strategic planning and programming cycle, audit coordination, monitoring and reporting on related processes and quality management are some of the key internal control activities in the EDPS.

In keeping with previous years, detailed information on activities carried out by the Data Protection Officer and by the Transparency Officer are provided, respectively, in chapters 10 and 11 of this Annual report.



CHAPTER TEN

The Data Protection officer of the EDPS



The focus of the Data Protection Officer (DPO) at the EDPS in 2023 was to enhance the EDPS' compliance and practice with 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).

To achieve this, the DPO continued to work together with the EDPS' services in charge of processing personal data with a view to ensure that the institution leads by example in upholding the highest standards of data protection.

The EDPS is an institution tasked with responsibilities that influence the lives, dignity and fundamental rights of all individuals in the EU, as well as their relationships with other people, private entities and public administration. With this in mind, the DPO contributed to strengthening the EDPS' accountability by raising the standard of data protection compliance of the ongoing and new personal data processing activities that the EDPS may need to carry out in its role as the DPA of EUIs, including seeking privacy and data protection friendly alternatives.

10.1.

Accountability

10.1.1.

Monitoring the application of data protection rules

The DPO constantly monitors the practical application of data protection rules and procedures in light of the legal provisions, case law and relevant guidance.

10.1.2.

Register for processing activities

The [EDPS' register of personal data processing activities](#) was regularly updated with new and updated records, which concerned various topics related to the EDPS' supervisory activities, IT, communication, administration and security.

10.1.3.

Updating data protection notices

As data controller, the EDPS aims to increase transparency and accessibility towards individuals and EDPS employees about how it processes their personal data.

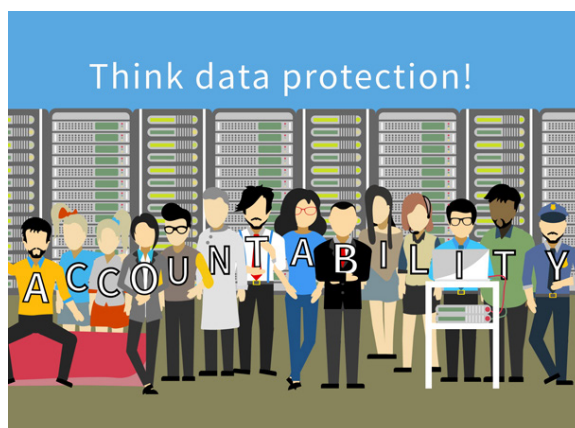
With this in mind, the EDPS continued to publish on its website and intranet new and updated data protection notices, sometimes in French, English and German, that are clearer and more comprehensive, in order to inform its viewers and readers on how their personal data will be processed for various purposes, such as the organisation of events, webinars, the use of social media, for example.

10.1.4.

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 the [EDPS Strategy 2020-2024](#).



10.1.5.

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.

10.2.

Advising the EDPS

The DPO continued to advise and work closely with services in charge of processing personal data in order to ensure the EDPS' compliance with data protection law and principles. In particular, the DPO counselled the EDPS on the data protection compliance of new services that the EDPS was considering to use, in the fields of human resources, information security and communication, for example.

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 as service providers to the EDPS; new and updated contracts with external service providers; and the review of certain internal rules and procedures.

10.3.

Enquires and complaints

10.3.1.

Enquiries

The overall number of enquiries and requests from individuals exercising their data protection rights received by the EDPS in 2023 increased in comparison to previous years.

2

Information requests

3

Rectification requests

11

Erasure requests

24

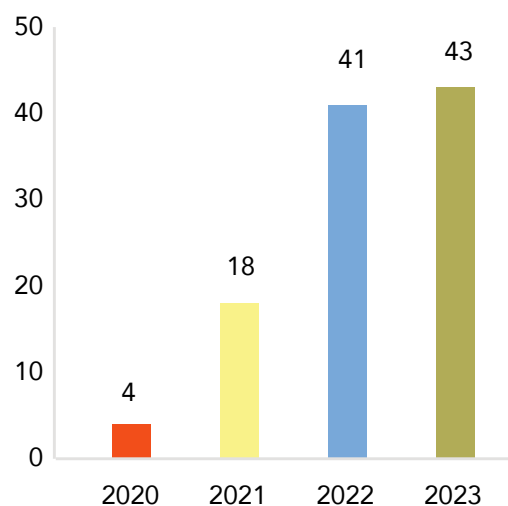
Inadmissible requests

4

Objection requests

23

Access requests



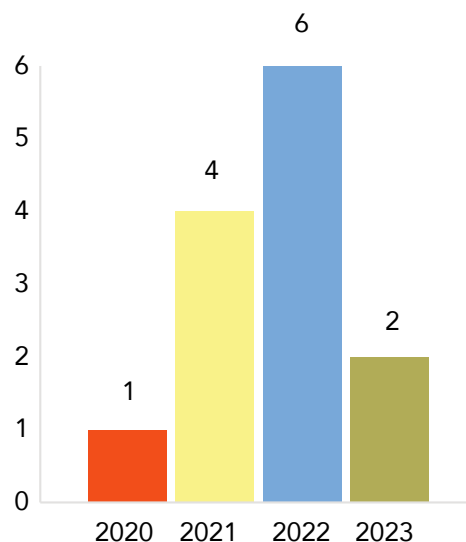
Evolution of data subject requests since 2020 (except inadmissible requests)

10.3.2.

Complaints

In 2023, the EDPS DPO received 2 complaints: 1 from an EDPS staff member and 1 from a citizen. The complaints concerned the processing of personal data related to communication purposes.

Individuals may lodge a complaint with the EDPS as a data controller, if they believe their data protection rights have been infringed by the EDPS when processing their personal data, for instances such as excessive amounts of personal data being collected; personal data being shared with third parties without appropriate legal basis.



Evolution of the number of complaints received by the EDPS DPO since 2020

10.4.

Raising awareness about data protection

In 2023, 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 regularly updated to take into account the latest developments in the field, including the most recent internal rules and procedures of the EDPS. Given the specificity of the EDPS, which, as a rule, recruits data protection specialists, particular attention is paid to tailor the content to the audience. As a result, presentations tend to focus more on internal rules and procedures, rather than general data protection concepts.

In order to raise awareness on data protection, the DPO also organised an artistic competition for Data Protection Day 2023, which gave the opportunity to EDPS staff to employ both their expertise in data protection and their unique artistic talents. EDPS colleagues appreciated this competition, as there was a variety of fascinating entries, focusing primarily on the interplay between data protection and AI. This competition is a way to reinforce collegiality between the EDPS staff, and to discuss data protection in a unique manner.

10.5.

Cooperation with other data protection officers

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.

As a well-established forum, the DPO participated in the EDPS' biannual meetings with the network of DPOs in May and November 2023. Similarly, the DPO also participated in regular meetings organised by the DPOs' network of the European Data Protection Board, made up of DPOs of national DPAs.

In order to foster cooperation and communication between the EDPS, as a DPA, and the EUIs' DPOs, two 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 transfers outside of the EU/European Economic Area, access to documents and data protection, EDPS piloting of open software.



CHAPTER ELEVEN

Transparency and access to documents



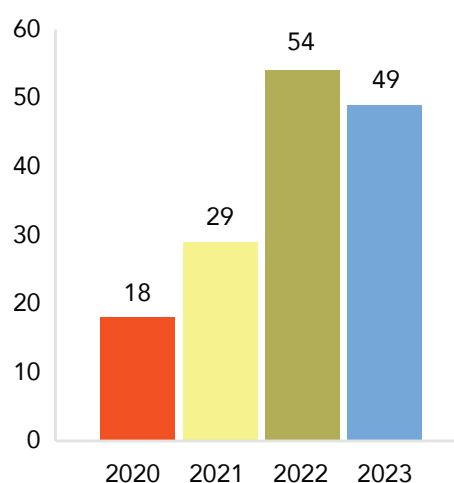
As an EUI, and according to our Rules of Procedure, the EDPS is subject to Regulation (EC) 1049/2001 on public access to documents.

Within the EDPS, the person responsible for handling these requests is a designated Transparency Officer. The appointed officer collaborates with the relevant staff members in order to respond appropriately to the requests.

In 2023, the EDPS received 49 access to documents requests. In five of these cases - 10% in 2023, against 5% in 2022 - we also received a confirmatory application. In all cases where documents could be identified, the requested documents were either fully or partially disclosed.

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, in 2023 the EDPS has examined the available options for joining the inter-institutional agreement on a mandatory transparency register.

Based on the analyses of the complex rules and procedures governing the Transparency Register, and taking into account the EDPS transparency state of play, the EDPS decided that it should take the necessary steps to adopt conditionality and/or complementary transparency measures and request the publication of such measures on the Transparency Register webpage.



Access to Documents requests since 2020



Publications Office
of the European Union

