EDPS

EUROPEAN
DATA PROTECTION
SUPERVISOR

ANNUAL REPORT

2022

An executive summary of the Annual Report 2022, which gives an overview of the key developments in EDPS activities in 2022, 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, 2023

PRINT ISBN 978-92-9242-717-7 ISSN 1830-5474 doi: 10.2804/451148 QT-AA-23-001-EN-C

PDF ISBN 978-92-9242-718-4 ISSN 1830-9585 doi: 10.2804/120286 QT-AA-23-001-EN-N

Table of contents

Foreword

I have the pleasure of sharing with you the EDPS Annual Report 2022. I look back on this year with a great amount of reflection. It has been an eventful year: challenging and hopeful, difficult yet encouraging - both for the world at large, and for the EDPS.

This year, with the Russian invasion of Ukraine, an unprecedented reaction was triggered from the European Union (EU). What the EU has proven over this last year is that it is capable of finding EU-wide solutions, especially in the face of external threat, in a way that not only proves solidarity but also upholds our key values and principles. It is in this spirit, that the EDPS has also aimed to demonstrate over the last year our commitment to upholding the fundamental right to data protection, even during moments of crisis where our measures and responses had to be swift and efficient. Our efforts to support EU lawmakers in the legislative process and supervise the development of Eurojust, the EU Agency for Criminal Justice Cooperation, are a testament to our belief that we are stronger together.

Despite such tumultuous global events, this year has also been one of aspiration and development - a moment to reflect on creating a tomorrow that can effectively tackle the challenges of today. Fully embracing the post-pandemic reality, we organised a conference in Brussels on 16-17 June, on "The Future of Data Protection: Effective Enforcement in the Digital World". With this conference, we gathered over 2000 participants, both in person and remotely, around one key objective: to foster progress in the debate on the future of enforcement of the General Data Protection Regulation, four years after its entry into application. I am proud of this event and the rich discussions that unfolded during our two-day conference, which triggered tangible actions in the data protection community. The European Data Protection Board's commitments reflected in its Vienna Summit Statement, or the European Commission's plans to propose a legislation harmonising certain procedural aspects of cross-border cooperation between data protection authorities, are two important examples of the effect that our conference has had. I look forward to seeing where this conversation leads us, and I am grateful to our community at large for their courage in these reflections.

As the data protection authority supervising the EU institutions, offices, bodies and agencies, the EDPS has the particular role of supervising exclusively public authorities. With this role comes a sense of responsibility to contribute to reflections on the function of the state in

a democratic society. This prompted us, for instance, to share our EDPS Preliminary Remarks on Modern Spyware as an attempt to create better democratic oversight over practices related to law enforcement or national security.

In this context, we also issued an EDPS Order to Europol to delete large datasets with no established linked to criminal activity. The legislative response to this matter and the subsequent EDPS application to the Court of Justice of the European Union to annul the retroactive provisions of the amended Europol Regulation is a sign of our deep belief that the European Union can - and should - be setting global standards concerning the rule of law and democratic values.

For this to happen, the highest standards should continue to be sought after in the EU itself. For the years to come, we remain committed to contributing to this important endeavour. I am sure that next year will bring its own challenges and revelations - but I look forward to tackling them, together with our dynamic and dedicated EDPS team.

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.

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**: We monitor the processing of personal data by EUIs to ensure that they comply with data protection rules.
- **Policy and Consultation**: We advise the European Commission, the European Parliament and the Council on legislative proposals and initiatives related to data protection.
- **Technology and Privacy**: We monitor and assess 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**: We work with data protection authorities to promote consistent data protection across the EU. Our main platform for cooperation with data protection authorities is the European Data Protection Board, to whom we provide a secretariat, and with whom we have a Memorandum of Understanding defining how we work together.

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 bodies 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; and EPPO - the European Public Prosecutor's Office under Regulation (EU) 2017/1939; as well as Frontex - the European Border and Coast Guard.

For more information about the EDPS, 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.

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 European institutions, bodies and agencies (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.

CHAPTER TWO

Going forward: our goals for 2023 and beyond

Mid-Term Strategy Review - 'Shaping a Safer Digital Future'

The EDPS 2020-2024 Strategy "Shaping a Safer Digital Future" was derived on the cusp of global change. Written in early 2020, it sets out three strategic focal pillars for the EDPS: **Foresight**, **Action**, and **Solidarity**. Yet even our best foresight experts could not have predicted the paradigm shift that was to follow. The COVID-19 pandemic, the war on Ukraine, and the global economic crisis, all formed part of the challenging environment that we were confronted with, following the adoption of our 2020 strategy.

This is why in 2022, we decided to conduct a mid-term review of our 2020-2024 strategy. Commenced with the intention of evaluating progress made on the objectives listed in the strategy, the mid-term review formed a crucial moment for considering whether a shift of institutional direction was needed in light of the changing global environment. The following chapter of the Annual Report presents the results of the mid-term review and sets out the EDPS' refocused vision and priorities for the remainder of the strategy.

Procedure of the mid-term review

A bottom-up approach to the mid-term review was implemented which saw the strategy's evaluation conducted from within. This decision was adopted with the intention of harnessing the fresh perspectives of the EDPS staff, bearing in mind the institutional growth that has taken place since 2020. This approach allowed us to leverage the in-house interdisciplinary knowledge and experience of the EDPS staff, to identify key focal areas for our work in the coming years.

The mid-term review was conducted in two stages. The first stage consisted of a gap analysis. This analysis was conducted on the basis of a mapping exercise which all EDPS staff took part in. This exercise was officially kick started through a discussion between the Supervisor and the EDPS staff, in which the Supervisor shared the planned procedure for open reflection and consideration of the staff. Following valuable input received at staff level, the mapping exercise was launched. The mapping exercise presented an overview of the 57 objectives listed in the EDPS 2020-2024 strategy on which the EDPS staff reflected on whether and to what extent objectives had been met. Following this preliminary assessment, a gap analysis was conducted to identify the state of progress of the objectives.

Results of the mapping exercise revealed the substantial progress that we made to implement and achieve the objectives listed in the strategy. Of the 57 objectives listed in the strategy, the gap analysis revealed that 15 objectives have been accomplished so far, 40 are ongoing, and only 2 are at an early process of implementation.

The positive results of the gap analysis formed the foundations for the second stage of the mid-term review. In this second consultative stage, the EDPS staff were consulted on the future of the EDPS and asked to consider how the new realities of our environment may warrant a shift in priorities for the remainder of the strategy. Specific attention was devoted to identifying focal areas which the EDPS would like to concentrate increased efforts on for the remainder of the strategy.

Outcomes of the mid-term review: from shaping a safer digital future, to championing its formation

The results of the consultation stage led to the emergence of several institutional priorities, which we consider to be key and we commit to dedicating additional attention and resources to, for the remainder of the 2020-2024 strategy.

Priority #1: Effective enforcement of data protection in a new regulatory landscape

With the adoption of multiple legislative initiatives in the digital field, the EDPS, together with the community of data protection authorities (DPAs), finds itself in a significantly more complex regulatory environment. This new regulatory landscape, which involves legislation such as the Data Governance Act (DGA), the Digital Markets Act (DMA) and Digital Services Act (DSA) on the one hand, and the proposed Artificial Intelligence Act and Data Act on the other, results in new regulatory functions and regulatory authorities being envisioned by the legislator.

Whilst these acts in principle state not to prejudice nor to amend the GDPR (or Regulation (EU) 2018/1725), several provisions in these new or forthcoming regulations explicitly refer to GDPR definitions, concepts and obligations. Moreover, whilst the processing of personal data is central to the activities regulated by each act, data protection authorities are not designated as the main competent authorities.

Enforcement is entrusted - either completely or to a very significant extent - to authorities whose missions primarily concern policy objectives other than data protection or privacy. Consequently, there is a need to ensure a coherent approach to regulatory activities across the digital sphere. We will therefore work to conceptualise our role regarding these authorities, and to identify the expectations of these authorities regarding the EDPS.

Building on its consolidated and widely acknowledged experience of ensuring a coherent approach in the digital ecosystem, we will therefore steer and actively engage in the work of relevant coordination forums provided for by law, such as the High Level Group of the DMA and other relevant coordination fora provided for by law, both as the EDPS and as a member of the European Data Protection Board (EDPB), as appropriate.

We will also actively promote strong cooperation with the relevant bodies in instances where a specific coordination body is not provided for by law, but where enforcement will require a close dialogue with the authorities tasked with applying provisions with privacy and data protection implications.

Moreover, we will strive to ensure that data protection principles and rules are not undermined by the application and enforcement of new legislation. The EDPS will therefore continue to engage in an advisory function in order to monitor and highlight potential consequences arising from the practical implementation of new regulatory frameworks. Enforcement action will also be considered where necessary.

It is within this context that the EDPS is also faced with its potential role as supervisory authority of the EU institutions, offices, bodies and agencies (EUIs) for Artificial Intelligence. Both from an organisational and a methodological perspective, intensive preparations are envisaged to ensure that we are ready to fulfil our new task from the beginning.

The Digital Euro project is also of high strategic importance to us and requires close cooperation amongst experts with policy, legal, technological and supervision expertise. Whilst much will depend on the design choices made, the Digital Euro project will undoubtedly have significant implications for privacy and data protection. Other proposals concerning the financial sector will also warrant close scrutiny, such as the legislative open finance framework proposal, which will aim to enable data sharing and third-party access for a wide range of financial sectors and products. We will therefore consider with utmost attention the possible interplay with the Data Governance Act and the Data Act.

The EDPS Conference held in June 2022 on "*The Future of Data Protection: Effective Enforcement in the Digital World*" triggered significant and much needed progress in the public debate on the enforcement of the General Data Protection Regulation (GDPR). The related developments, in particular the so-called EDPB Vienna Statement, and the announced proposal of the European Commission for a Regulation harmonising certain aspects of national procedural rules, show that efforts on the potential improvements to the functioning of the GDPR will continue to dominate the debate in the years to come. The success of the EDPS Conference, in terms of public interest and impact, shows there is a significant role for the EDPS, as an independent EU institution, in this debate to advocate for pan-European approaches that ensure that the EU Charter of Fundamental Rights is respected fully.

Priority #2: Interoperability as a challenge requiring an overhauled supervisory approach

With the onset of interoperability, the EDPS is facing substantial obligations to ensure an effective supervisory approach. With the introduction of the EU's interoperability framework which adopts a new approach to the management of data for borders and security, we are subsequently also rethinking its methodology for the supervision of large-scale IT systems. The proposed interoperability changes by the EU's framework would see the linking of several large-scale IT systems with the Europol and Interpol databases, which would constitute a data flow ecosystem that amplifies the risks to data subjects generated by the operation of the underlying systems.

There are several challenges that we have identified that will need to be addressed. The complexity of the overall architecture and fragmentation of data protection rules calls for recalibrated supervision which focuses on data flows, rather than on the separate monitoring of data processing in different systems. Similarly, the introduction of additional data processing activities that were not initially laid down in the legal instrument regulating the establishment of each of the underlying large-scale IT systems calls for thorough scrutiny of the purpose limitation principle. Moreover, there may be decisions taken that have a substantial impact on data protection related to comitology procedures and transfers of responsibilities to the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). The absence of a single channel through which to exercise data subject rights simultaneously across all systems may lead to a fragmentation of these rights.

The EDPS will therefore focus on the following three priority areas, which will form a basis for our supervision of the interoperability framework until the end of the mandate:

(1) Data subject rights - Aiming at addressing the risk of fragmentation of data subject rights with the variety of interoperable databases with multiple controllers, we will explore the potential for coordinated supervision (including joint reflection with DPAs on streamlining procedures for data subjects' rights). In addition, we will aim to develop a proactive approach to data subject rights, in particular the right to information.

(2) Audit strategy - Developing a tailor-made strategy for data protection audits in the large-scale IT systems and the interoperability components, adapted to the new ecosystem, possibly constituting a shift from auditing siloed systems to data flows. The strategy will include a joint approach to auditing interoperability by taking into account further auditing obligations towards EU Agencies (Europol, Frontex, Eurojust), in order to safeguard purpose limitation and verify that those entities are accessing and processing data in line with their respective mandates. This joint approach will contain a legal and a technical part. Furthermore, since the large-scale IT systems' regulations explicitly request the EDPS to perform "*audits in accordance with international audit standards*", a common interpretation of this requirement will be necessary.

3) Algorithmic profiling - Work on algorithmic profiling will aim in particular to position the EDPS regarding the application of this tool within the interoperability framework (ETIAS and VIS) and more generally focusing in particular on issues of discrimination, reliability, proportionality, and transparency. The supervision of algorithmic profiling is a complex issue that is only at early stages and requires cooperation with other agencies and bodies in the field of human rights and non-discrimination, and possibly other actors from civil society and academia. Such supervision will support our input to the work of both the ETIAS - the European Travel Information and Authorisation System and Visa Information System Fundamental Rights Guidance Boards and will aim to develop appropriate monitoring and supervisory tools for this new area of supervision.

Priority #3: International cooperation to promote global common approaches on privacy and data protection challenges

We consider that actively engaging in international cooperation is of fundamental importance. Doing so allows us to engage with a wider community, beyond Europe, and to promote a common understanding and approaches towards data protection and privacy challenges. We plan to further increase our efforts in the field of international cooperation, as several topics of high strategic importance are discussed in international fora.

In particular, we intend to foster coordination of the actions and strategy of EDPB members in international fora, further engage in the work carried out in the context of the GPA - Global Privacy Assembly, the Council of Europe, as well as within the G7 DPAs Roundtable, and the OECD - Organisation for Economic Co-operation and Development, by ensuring active participation and effective representation of European authorities' and EDPB's views. We will also aim to further step up cooperation with international organisations as well as with regional data protection networks.

Priority #4: Rethinking EDPS processes to ensure efficiency in a fast-changing environment

The EDPS 2020-2024 strategy is being implemented in a period in which crises have occurred one after another. From the COVID-19 pandemic, to the Russian invasion of Ukraine, to rising energy and inflation costs, we have had to adapt our working methods and processes in order to continue delivering on our output. Whilst we have managed to deliver, in principle, on the commitments made in the strategy, internal analysis shows a need to further readjust approaches to certain processes, with the aim of improving our efficiency and long-term standards, both as an EU public administration and as a data protection authority.

In the latter case, this relates, amongst others, to deliverables such as following up on data breach notifications, resolving complaints, or the ability to proactively target critical compliance-related topics via investigations or audits. Further reflection on new tools allowing online or remote assessment of compliance will take place. At the same time, human resource and budgetary constraints pose a significant obstacle for the fulfilment of the EDPS supervisory tasks.

In the same vein, the war in Ukraine brings new stand-alone tasks to the EDPS. In 2021, the European Commission proposed a legislative package to amend the Eurojust Regulation to allow for the processing of evidence collected for the purpose of investigating war crimes committed by Russia. In 2022, another legislative amendment was passed, designating Eurojust as the European hub for preservation, storage and analysis of evidence on core international crimes. We have been attributed an important role in the setting up of the new evidence database. In January 2023, the European Commission announced the creation of the International Centre for the Prosecution of the Crime of Aggression (ICPA) at Eurojust. All these legislative changes have already resulted or will result in substantial additional tasks for us. Given the political importance of the EU's support to Ukraine, as well as the considerable workload attached to it, our activities in this area will be recognised as one of our key priorities.

With the increasing public interest in the work of the EDPS, as shown by, amongst others, the number of access to documents requests, we also commit to higher standards of transparency, not only as part of good administration, but also as an important way of making our work accessible to individuals. We also commit to continuing to ensure high levels of data protection and accountability, and to lead by example not only by complying with legal requirements, but also by exploring and making use of first-rate privacy and data protection-friendly tools and services. Concerning cybersecurity, we will have to adapt to new regulations aimed at ensuring a high common level of cybersecurity across the EUIs.

CHAPTER THREE

Our 2022 Highlights

3.1.
Using our powers to protect individuals

As the data protection authority in charge of supervising the EU institutions, bodies, offices and agencies (EUIs), our goal is to ensure that they comply with EU data protection law, to protect individuals and their fundamental rights to privacy and data protection.

To help achieve this, we provide EUIs with guidance, issue recommendations, remarks and Opinions, carry out audits, offer training sessions, as well as other resources to equip them with the suitable tools to put data protection into practice throughout their day-to-day tasks, decisions or measures requiring the processing of individuals' personal data.

3.1.1.
Supervising the Area of Freedom, Security and Justice

Amongst the topics on which our intervention was needed, particular focus of our work permeated to supervising the EU's Area of Freedom Security and Justice (AFSJ), which covers policy areas ranging from the management of external borders, judicial cooperation in civil and criminal matters, as well as asylum, migration, combatting crime. AFSJ includes EU Agencies, such as Europol - the EU Agency for law enforcement cooperation, Frontex - the EU Border and Coast Guard Agency, EPPO - the European Public Prosecutor's Office, Eurojust - the EU Agency for Criminal Justice Cooperation. Therefore our role in this area was particularly important, given the sensitive nature of the information being processed, and the considerable impact this may have if mishandled. (See Section 4.7)

3.1.2.

Transfers of personal data to non EU/EEA countries

The topic of international transfers of personal data to countries outside the EU or the European Economic Area (EEA) also commanded our attention increasingly over the years, including in 2022, demanding us to mobilise substantial resources so that the level of protection of individuals' personal data is ensured.

To this end, we carried out a certain number of initiatives, and provided advice and recommendations on how EUIs should meet the requirements of EU data protection law when using services or entering into contracts with entities located outside the EU/EEA. (See Section 4.5)

The use of non-EU/EEA products and services

Our initiatives include our ongoing investigations into EUIs' use of products and cloud services from entities based outside the EU/EEA, in particular the European Commission's use of Microsoft Office 365, the issuance of guidelines and policies, as well as providing trainings to EUIs. These efforts aim to raise EUIs' awareness of the risks posed by using tools or conducting data processing activities that imply transfers of data outside the EU/EEA. We also aim to raise EUIs' awareness of the contractual clauses and administrative arrangements, as well as other measures to put in place to ensure that individuals' personal data is protected in an essentially equivalent way outside of the EU/EEA.

As part of our work in this area, and in light of our EDPS powers, we authorised a number of transfers of personal data to non-EU/EEA countries, where EUIs were able to prove robust procedures and safeguarding measures to ensure that these transfers guaranteed the protection of individuals' personal data.

With the aim of leading by example in this field, we are also working towards using alternative products and services that are based in the EU/EEA, and we are encouraging EUIs to consider this as well.

3.1.3.
Auditing Large-Scale IT Systems

One of our key roles is to ensure the protection of personal data and privacy in the context of large-scale IT systems in the Area of Freedom, Security, and Justice. One of our functions is to audit these systems to ensure that they comply with data protection and privacy regulations.

In carrying out our auditing function, we evaluate the technical and organisational measures put in place by system operators, ensuring that systems are designed with privacy-by-design principles. We also promote best practices by sharing findings and recommendations from audits with other EU data protection authorities, fostering a culture of excellence in data protection and privacy across the EU.

With our auditing activities, we work to raise awareness amongst EUIs and the general public about the importance of data protection and privacy in large-scale IT systems. By fulfilling this vital role, we help safeguard the personal information of EU citizens and ensure that large-scale IT systems adhere to the highest data protection and privacy standards.

In October 2022 we carried out an onsite audit of three large-scale IT systems, at eu-LISA - European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice's premises in Strasbourg:

Eurodac, the European Asylum Dactyloscopy Database, which assists in the processing of asylum applications.

SIS II, which supports internal security and the exchange of information on individuals and objects between national police, border control, customs, visa and judicial authorities.

VIS, which supports the application of the EU common visa policy and facilitates border checks and consular cooperation.

The audit included the review of methodology and practices eu-LISA employs to develop and test systems whilst ensuring that security and data protection by design and by default principles are applied. Additionally, we audited the measures related to IT Security Governance, security incidents and personal data breaches, and we checked the application of the recommendations from our previous audits.

3.2.
Protecting our independence

New Europol Regulation: EDPS legal action in the Court of Justice of the European Union

On 16 September 2022, we requested that the Court of Justice of the European Union (CJEU) annuls two provisions of the newly amended Europol Regulation, which came into force on 28 June 2022 (Case T-578/22 – EDPS v Parliament and Council). The two provisions have an impact on personal data operations carried out in the past by Europol. In doing so, the provisions seriously undermine legal certainty for individuals' personal data and threaten the independence of the EDPS.

3.3.
Shaping a safer digital future

As set out in our EDPS Strategy 2020-2024, we value initiatives where data generated in Europe is converted into value for European companies and individuals, and processed according to European values, to shape a safer digital future. Following this direction, we provided advice to the EU legislator on a wide range of matters: health, artificial intelligence, initiatives to help combat crime, for example.

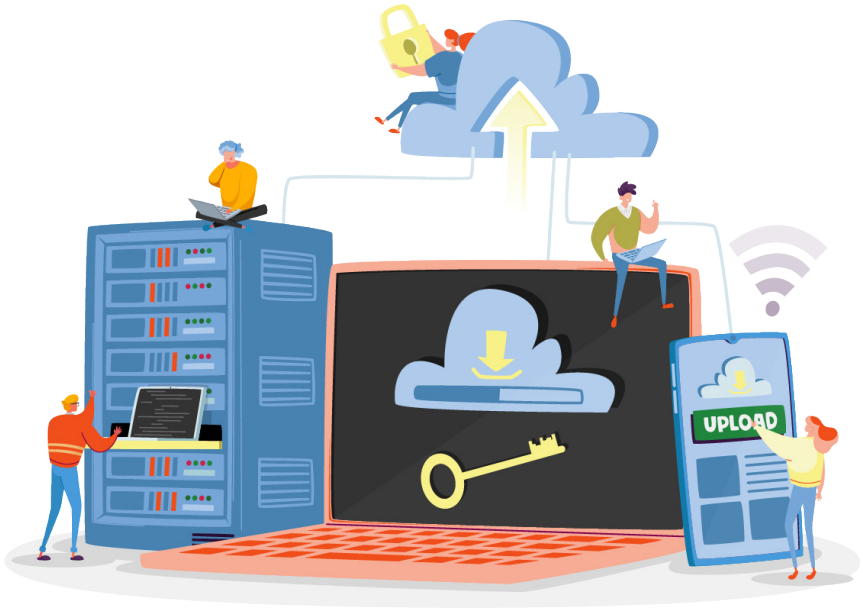
We normally provide advice to the EU legislator on proposed legislation in the form of Opinions or Formal Comments. Our **Opinions** are issued in response to mandatory requests by the European Commission, which is legally obliged to seek our guidance on any legislative proposal, as well as recommendations and proposals to the Council in the context of international agreements with an impact on data protection. **Formal Comments** are issued in response to a request from the European Commission on draft implementing or delegated acts.

Where a legislative or other relevant proposal is of particular importance for the protection of personal data, the European Commission may also consult the European Data Protection Board (EDPB). In such cases, the EDPS and EDPB work together to issue a **Joint Opinion**. (See Chapter 5)

The EU Data Act

We issued a Joint Opinion with the EDPB on the proposal for the Data Act, which aims to establish harmonised rules on the access to, and use of, data generated from a broad range of products and services, including connected objects ('Internet of Things'), medical or health devices and virtual assistants.

The Opinion highlighted that data must be processed according to European values if we aim to shape a safer digital future. As new opportunities for data use are created, it must be ensured that the existing data protection framework remains fully intact. We also underscored that access to data by public authorities should always be properly defined and limited to what is strictly necessary and proportionate, which is not the case under the draft Data Act. (See Section 5.2)



The European Health Data Space

We also issued a Joint Opinion on the Proposal for the European Health Data Space in which we advocated for strong protection of electronic health data.

The Proposal for the European Health Data Space is the first of a series of proposals for domain-specific common European data spaces. It will be an integral part of building a European Health Union aiming at enabling the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data.

Together with the EDPB, we expressed several concerns, notably on the secondary use of electronic health data. (See Section 5.3)

Artificial Intelligence

As highlighted in our EDPS 2020-2024 Strategy, Artificial Intelligence (AI) is increasingly deployed in public services and criminal justice. Our role is to ensure that this new technology is used in compliance with EU data protection law and respects individuals' privacy.

In addition to other initiatives we have produced, or participated in, we issued an Opinion on the Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law (AI Convention), which we consider as an important step to develop the first legally binding international instrument on AI according to the European standards and values on human rights, democracy and the rule of law, complementing the EU Artificial Intelligence Act. Nevertheless, we highlighted the need to include appropriate, strong and clear data protection safeguards to protect individuals who may be affected by the use of AI systems.

Combatting crime

We issued a selection of Opinions on diverse Proposals in the field of criminal law.

For example one of our Opinions, jointly issued with the EDPB, focused on a proposed Regulation to prevent and combat child sexual abuse (CSAM). We expressed support to the goals and aims of the Proposal, whilst, however, expressing concern that it may present more risks to individuals, and, by extension, to society at large, than to the criminals pursued for CSAM (See Section 5.4).

Another notable example where we provided our recommendations and guidance concerned the topic of international cooperation to fight crime. In particular, we issued an Opinion on two Proposals: one to authorise EU Member States to sign the Second Additional Protocol to the Budapest Convention on Cybercrime, and the other to authorise EU Member States to ratify this same Protocol.

Whilst investigating and prosecuting crime is a legitimate aim, for which international cooperation, including the exchange of information, plays an important role, we emphasised the importance for the EU to have sustainable agreements for sharing personal data with non-EU countries for law enforcement purposes. These agreements should be fully compatible with EU law, including the fundamental rights to privacy and data protection.

3.4.
The Future of Data Protection: Effective Enforcement in the Digital World

In June 2022, we organised our EDPS Conference, titled "The Future of Data Protection: Effective Enforcement in the Digital World", which brought together over 2,000 participants, both in Brussels and online. Featuring over one-hundred speakers; three main sessions; sixteen breakout sessions; nine individual keynote remarks; and five side events. The two-day event fostered crucial conversations on the future of data protection, with a particular focus on the enforcement of the General Data Protection Regulation (GDPR).

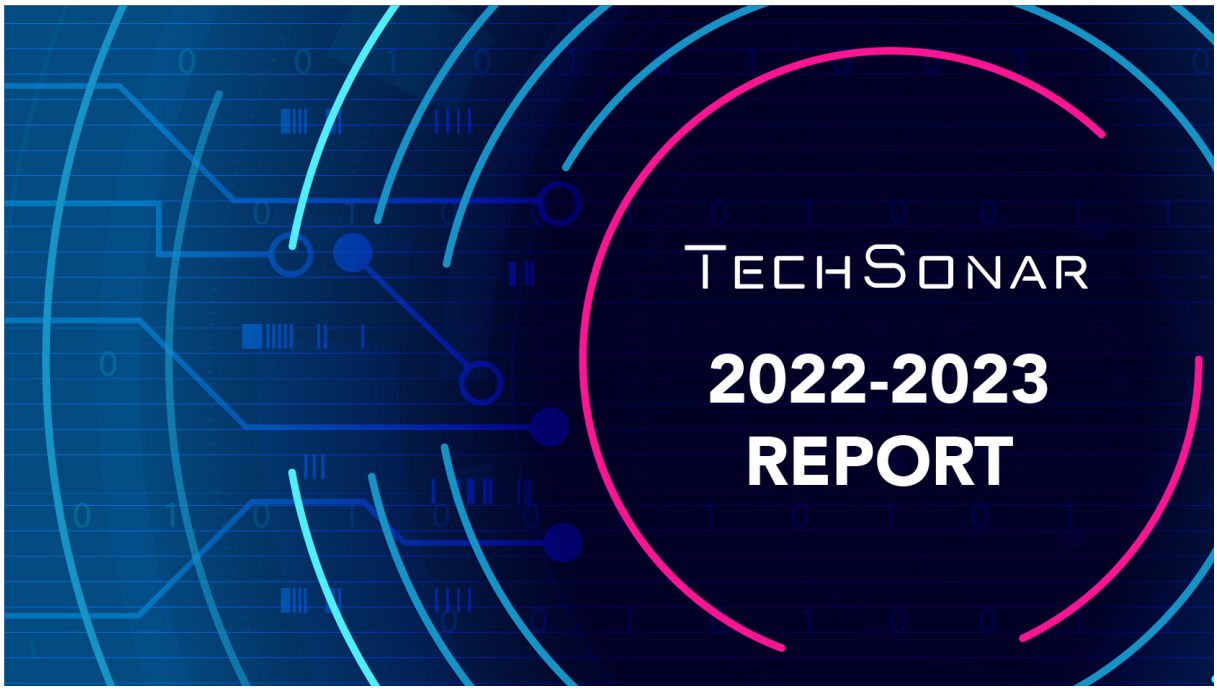
Our long-term vision for the future of data protection is clear: it is necessary to approach enforcement in a pan-European way to ensure real and consistent high level protection of individuals and to deliver the promise of the GDPR. (See Chapter 8)

3.5.
Technology Monitoring & Foresight

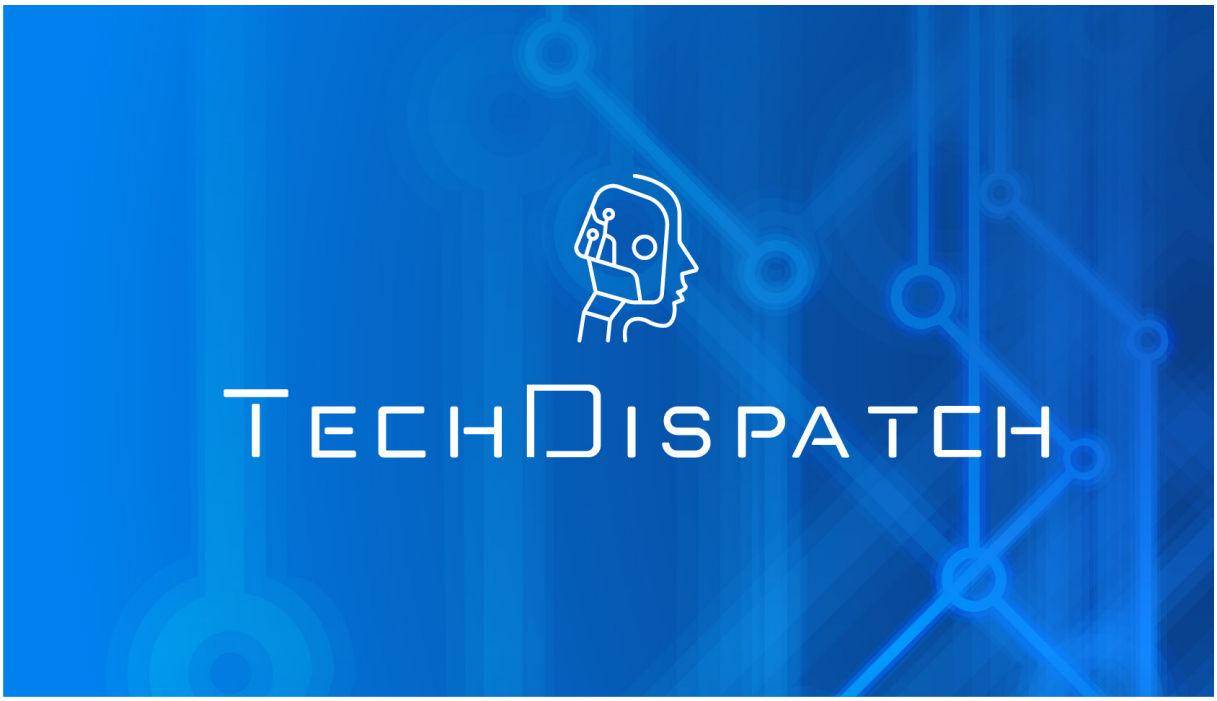
One of the three core pillars of the EDPS strategy for 2020-2024 is **foresight**, namely, our commitment to being a smart institution that takes the long-term view of trends in data protection and the legal, societal and technological context.

One of the ways we put foresight into practice is to engage with experts, specialists and data protection authorities. We aim to understand technologies, analyse their privacy and data protection implications on individuals, with the aim of sharing knowledge and nudging the development of these new and emerging technologies in a privacy-compliant way. **TechSonar** and **TechDispatch** are two of our initiatives in this area.

TechSonar aims to anticipate emerging technology trends. The main aim of this initiative is to better understand future developments in the technology sector from a data protection perspective. Based on our collective effort, via scouting of trends, brainstorming, review, publishing, advocacy and continuous monitoring, we aim to contribute to the wider debate on foresight within the EUIs. Published on 10 November 2022, the second annual TechSonar report delves into five technologies worth monitoring this upcoming year. These are: central bank digital currency; metaverse; synthetic data; federated learning; and fake news detection systems. (See Section 6.1.1)



TechDispatch aims to explain emerging technology developments. The TechDispatch reports, for which we won a Global Privacy Assembly award in 2021, are part of the wider EDPS activities on technology monitoring. Each TechDispatch provides factual descriptions of a new technology, preliminarily assesses possible impacts on privacy and the protection of personal data, as we understand them now, and provides links to further recommended reading. This year's TechDispatch, published in July 2022, focuses on Fediverse and Federated Social Media Platforms. (See Chapter 6)

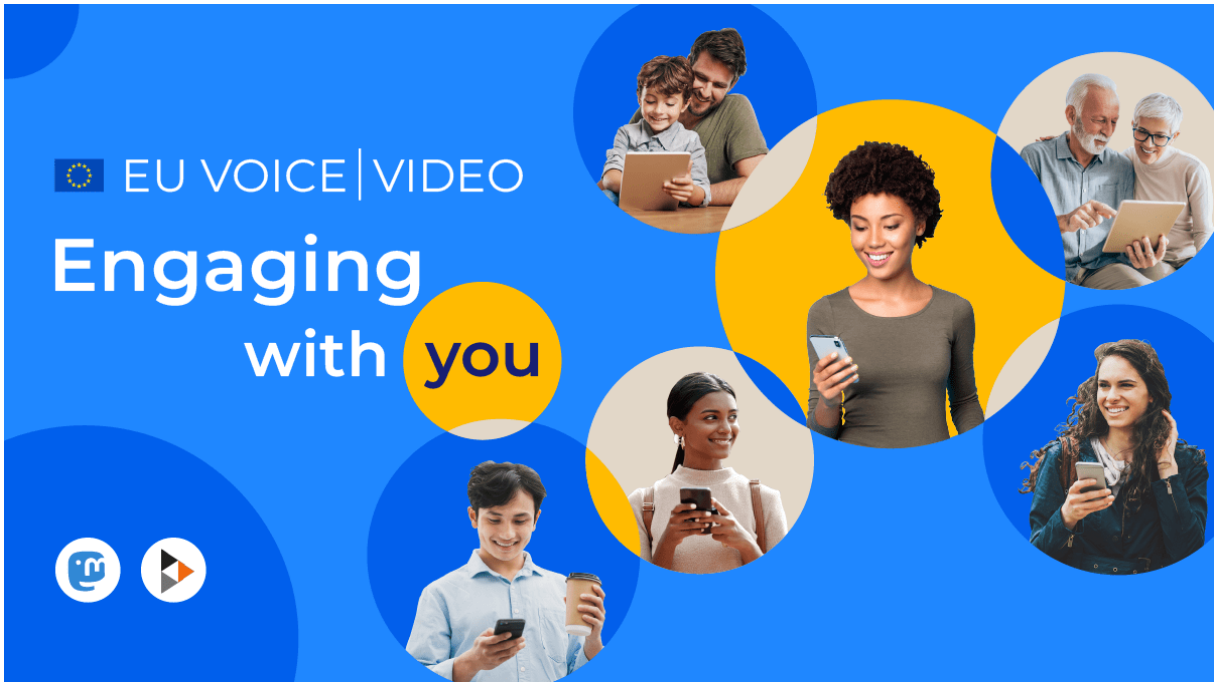


3.6.
Digital Innovation

Promoting data protection friendly tools that respect, and prioritise, individuals' fundamental rights throughout their development and use is one of our core aims of the EDPS Strategy 2020-2024. To match these objectives, we have sought, and continue to seek, alternative tools, particularly communication and collaborative tools, that comply with EU data protection laws and standards. By using these alternative tools ourselves, we aim to encourage EUIs to follow our example. This way, we can collectively minimise our reliance on monopoly providers, to avoid detrimental lock-in.

We play a significant role in promoting digital innovation by leading by example, for example by using open-source applications and platforms that offer privacy-friendly alternatives to products and services provided by big tech companies. Our commitment to privacy extends to both social networks and collaboration tools, with initiatives such as EU Video, EU Voice, and the pilot Nextcloud projects.

In February 2022, we launched the pilot phase of two social media platforms: EU Voice, to publish regular posts on our activities, and EU Video, to publish videos, as additional, alternative, communication channels to interact with our audience. Both platforms are part of decentralised, free and open-source social media networks that connect users in a privacy-oriented environment, based on Mastodon and PeerTube software. Both projects emphasise data protection and user privacy, ensuring that EUIs have access to communication tools that align with European values and principles, without compromising their personal information.



In addition to social networks, we support the adoption of alternative collaboration tools that prioritise privacy. The pilot Nextcloud project is a prime example of this commitment. Nextcloud is an open-source, self-hosted cloud platform that allows users to securely store, share, and collaborate on files, calendars, and contacts. By promoting and using privacy-conscious tools like Nextcloud, we demonstrate a commitment to fostering a digital ecosystem that upholds data protection and privacy principles, ultimately encouraging the development of innovative and more privacy-friendly alternatives.

In June 2022, during the EDPS conference "The Future of Data Protection: Effective Enforcement in the Digital World", we also developed a bespoke videoconferencing solution which fully respected the data transfer requirements under the GDPR and Regulation (EU) 2018/1725, allowing us to lead by example and pave the way for compliance with data protection requirements. As the data protection authority competent for supervising all EUIs, it was important to us to show that it is possible to demonstrate exemplary compliance when it comes to videoconferencing tools, and in particular to comply with data transfers rules when it comes to transferring personal data to countries outside of the EU and EEA. (See Chapter 8)

3.7.
Communicating data protection

Explaining what we are doing and why, in a transparent, clear, and interactive way is part of our goals as an organisation, because it is important for EU citizens to understand their data protection rights, and how these may be impacted.

An increasingly growing online presence

The EDPS has a well-established online presence on several social media channels, namely Twitter (29,1k), LinkedIn, where we have exceeded 63.000 followers this year, YouTube (2,75k), EU Voice (5,1k) and EU Video (0,69k) with which we are able to us to reach a global audience easily and quickly.

At large, we create content to promote visibility-enhancing campaigns and also live-reporting of the EDPS' participation in events.

Bringing data protection closer to the public

Data protection can be quite complex at times; hence, we put our effort to issue content that suits both experts and non-experts in data protection matters, bringing our work closer to the public.

This includes producing monthly newsletters, providing short, bite-size explanations about our latest initiatives and how these may impact the public; producing factsheets, in which we break down key data protection concepts, as well as executing social media campaigns, and collaborating with other EUIs to raise awareness on data protection matters. Going further in this direction this year, we launched a new podcast series, Newsletter Digest, to reach out to a larger audience, informing them about what we do to protect their data.

Media and Public Relations

We frequently interact with the media, especially through our press releases on significant data protection initiatives having a wide impact across the EU. This year, several topics garnered the most attention, with follow-ups or interview requests, such as the supervision of Europol and Frontex, or our EDPS Conference in June.

Likewise, we maintain our relationship with the public, by addressing public requests on our work and competences as an EU institution, and by organising study visits in our premises.

Picking up the pace after COVID-19

As the COVID-19 restrictions were gradually minimised, we were able to resume events, increase in-person activities, whilst still adapting these events to a post-COVID world. Our events and activities were designed for both online and in-person attendance; at the same time, this helped us reduce our environmental impact as an organisation. Markedly, we successfully hosted two large hybrid events: the Conference on "The Future of Data Protection: Effective Enforcement in the Digital World" in June 2022, hosting 2000 people both online and in-person, and our "Supervision Conference: Data protection and criminal justice" in November 2022, with over 200 people both online and in-person. For most of our events, we have put our best foot forward to go "greener" by sourcing from local catering, avoiding food waste and sourcing our brand material locally and made from reusable materials.

Collaborative Communication

In 2022, we have worked with other EUIs, collaborating on common communication activities. In October, we joined forces with ENISA - the European Union Agency for Cybersecurity, and the European Commission, to put forward a campaign for the European cybersecurity month (ECSM), marking its 10th anniversary. In another instance, we provided ideas and support in data protection matters for the purposes of inter-institutional online communication (IOCC). In particular with EU Voice and EU Video pilot project, we extensively cooperated with IOCC in order to provide editorial guidelines and servers' policies as well as to help EUIs taking part in the project.

3.8.
An evolving organisation

To support our objectives, in particular those set out in our EDPS 2020-2024 Strategy, we have expanded our organisation, and made other changes to better reflect our way of working.

We adjusted the internal organisation of the EDPS, creating a dedicated Legal Service, and the Governance and Internal Compliance Sector, to bring about the necessary expertise to be able to carry out certain tasks.

Delivering on our goals also means that we must manage our resources carefully. In this respect, substantial effort was invested in the planning, executing and auditing our budget.

We also made the necessary preparations to open an EDPS liaison office in Strasbourg, which will be officially inaugurated in early 2023, to reinforce inter-institutional and international cooperation, and to be able to provide additional advisory support on data protection matters.

Key Performance Indicators 2022

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 allows us 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 2022. These results are measured against initial targets, or against the results of the previous year, used as an indicator.

In 2022, we met or surpassed - in some cases significantly - the targets set in eight out of nine KPIs, with one exception being KPI8 - Occupancy rate of the establishment plan. These results illustrate well the positive path we have kept in implementing our strategic objectives throughout the year.

KEY PERFORMANCE INDICATORS		Results 31.12.2022	Target 2022
KPI 1 Internal Indicator	Number of initiatives, including publications, on technology monitoring and on promoting technologies to enhance privacy and data protection organised or co-organised by the EDPS	13 initiatives	10 initiatives
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 EDPS has provided a substantial written contribution	27 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	21 cases	5 cases
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	4 Joint Opinions 27 Opinions	Previous year as benchmark

KPI 6 External Indicator	Number of audits/visits carried out physically or remotely	4 audits + 1 visit	3 different audits/ visits
KPI 7 External Indicator	Number of followers on the EDPS social media accounts on YouTube (YT), LinkedIn (L), Twitter (T), EU Voice, EU Video.	Twitter: 29.1k LinkedIn: 63k YouTube: 2.75k EU Voice - 5.1k EU Video - 0.69k	Results of previous year + 10%
KPI 8 Internal Indicator	Occupancy rate of establishment plan	86,9%	90%
KPI 9 Internal Indicator	Budget implementation	98,2%	85%

CHAPTER FOUR

Putting data protection into practice

Our overarching aim as the data protection authority of EU institutions, bodies, offices and agencies (EUIs) is to ensure that they comply with the applicable EU data protection law, Regulation (EU) 2018/1725, so that individuals' fundamental rights to privacy and data protection are duly respected.

To help achieve this, we provide EUIs with guidance, recommendations, training sessions and other resources, to equip them with the adequate tools to put data protection into practice throughout their day-to-day tasks, decisions or measures requiring the processing of individuals' personal data.

Whilst we share advice with EUIs on many different topics, special focus this year was put on adapting our guidance regarding COVID-19's evolving situation, activities involving transfers of personal data outside the EU/European Economic Area (EU/EEA), cooperating with EUIs' data protection officers, to name a few examples.

We also placed particular importance on holding EUIs accountable for their actions impacting privacy and the protection of personal data, by conducting investigations, addressing complaints and carrying out audits, when and if necessary.

4.1.
COVID-19: monitoring data processing activities

In 2022, we continued to provide EUIs with the support they needed to adapt their measures related to COVID-19 as the situation evolved, by, for example, helping them make an inventory of the measures introduced during this health crisis to ensure that these are temporary, thus avoiding excessive collection of individuals' personal data that may no longer be necessary.

4.1.1.
Adapting and updating our guidance

In March 2022, we published a report on the new processing operations and IT tools that EUIs introduced during the COVID-19 pandemic to ensure business continuity. This included, for example, IT tools used or enhanced by EUIs to enable teleworking, new processing operations put in place by EUIs in charge of tasks related to public health. Our report notably addressed compliance of these activities with Regulation (EU) 2018/1725.

We published this report with acknowledgement that the dynamic evolution of a global health crisis, such as COVID-19, means that EUIs have had to continually adapt their processing operations. With this report, we aimed to support them in what appeared to be a long-lasting challenge, which will likely continue to have an impact in the coming years. Adoption of this report enabled us to provide further guidance to EUIs with regard to data protection aspects that deserve closer consideration. Indeed, reporting on EUIs' activities allowed us to take stock of issues, actions and progress made during the pandemic.

The results of the survey, displayed in the report, also play a vital role in informing our work and fed into our mission of updating and developing guidance for EUIs and their respective data protection officers, to ensure that individuals' personal data is protected.

4.1.2.
Data protection implications of COVID Passes

In 2022, we also continued to deliver a number of Opinions on matters related to COVID-19.

The use of COVID certificates and passes, to access EUIs' buildings for example, and the implications that these may have on individuals' data protection, remained a topic where our guidance was needed. We delivered three Supervisory Opinions covering this issue, in which we highlighted the importance of ensuring that measures introduced during a global health crisis, like COVID-19, should be limited in time and only to the extent that they are necessary and proportional in light of the objectives pursued, especially given the increase of data collected during COVID-19. We also made it clear that personal data initially collected for the management of this health crisis should not be repurposed for other objectives. EUIs should also review the evolution of the epidemiological situation, and modify or abort their measures accordingly.

In our Opinion concerning the verification of COVID-19 certificates in Luxembourg, we urged the European Commission (EC) to review whether extending the verification of COVID-19 certificates to individuals who are neither staff members, nor visitors of their premises, was necessary and proportional. Furthermore, we recommended that additional information is included in the draft Decision concerning the application of appropriate safeguards for carrying out and verifying COVID-19 self-diagnostic tests.

We also issued an Opinion on the requirements of using a Super Green Pass to access the Joint Research Centre (JRC) site. We advised the EC to assess and document whether it is necessary and proportional to use this pass to enter the JRC.

Recommendations were also submitted to the European Parliament (EP) in response to the EP's decision to extend the use of the EU Digital COVID-19 certificate (EUDCC) to all individuals entering the EP's building. In particular, we asked the EP to further clarify the circumstances and modalities in which a manual verification of the EUDCC may take place, under the institution's internal decisions. In addition to assessing whether national health and safety legislation is applicable, we recommended that the EP verifies if appropriate technical and organisational measures were put in place, in line with the Regulation (EU) 2018/1765, to protect individuals' health data.

4.1.3.
Sensitive information: processing health data

We also adopted an Opinion on the processing of certain health data related to medical vulnerability and COVID-19, by the European Investment Bank's (EIB) Occupational Health Service.

Given that individuals' health information is sensitive, we reminded the EIB that this type of data can only be processed for specific reasons, such as public health, and that if processed, the EUI should put in place suitable and specific measures guaranteeing that the processing is done in a secure way.

We also highlighted that the processing of health data should be conducted in a transparent and fair way, by providing clear information to individuals about how their health data is processed, for example. Complementing our other recommendations, we advised that this data should only be processed by staff bound by professional secrecy.

4.2.
Protecting individuals' personal data in EUIs

Whether EUIs outsource some of their activities, conduct recruitment procedures or any other initiatives, we support them to cultivate a mindset of treating the protection of individuals' personal data as a priority, by providing them with tailored advice when we are consulted on specific matters, or when we deem it necessary.

4.2.1.
Outsourcing activities: defining data protection responsibilities

When outsourcing certain activities, EUIs may face several data protection implications.

In such cases, EUIs may be confronted with issues of responsibility, such as defining who is responsible for the purpose, type and means of processing personal data - known as controllers, and who is responsible for processing personal data - known as processors. This information, as well as the circumstances in which personal data may be processed, must be known to the concerned EUI to ensure the protection of individuals.

Against this background, EUIs often request our advice on whether external service providers should be considered as joint or separate controllers, or processors.

For example, we issued an Opinion in April 2022 regarding the status of legal advisers and other private services procured by the European Investment Bank (EIB). We recommended that, in order for private service providers to only act as processors, and for the EIB to maintain control over these processing operations, detailed instructions on the processing of personal data should be provided by the EIB. Additionally, in its capacity as controller, the EIB must ensure that contracts governing the processing activities include the responsibilities and tasks of the processor, as well as information on individuals' data protection rights.

In two other of our Opinions, we advocated that an EUI should not be considered as a controller when processing is carried out by an external service provider, when the latter is subject to specific legal requirements regarding the processing of personal data.

Ultimately, the qualification of a service provider as a controller or processor should be the result of careful consideration by the EUI on the role it aims to and must play, depending on the nature, scope, context and purposes of the processing.

4.2.2.
Restricting individuals' rights

We issued a Supervisory Opinion, in October 2022, on the processing of personal data for historical archives by the European Central Bank (ECB), the EU institution in charge of supervising banks and the financial system of the EU.

Under EU data protection law, EUIs are allowed to derogate from certain data protection rights of individuals, for example when personal data is processed for archiving purposes in the public interest, subject to certain conditions.

The EDPS' main recommendations included in its Supervisory Opinion are the following:

- the ECB should ensure that it provides information to individuals about the subsequent transfer of their personal data to the historical archives at the same time as providing information about the processing of their personal data when it is initially collected;
- the ECB should clarify certain concepts, such as the concept of "sensitive personal data" envisaged for processing;
- contrary to what the ECB currently envisages, the right to data portability - a right that gives an individual the possibility to receive their personal data in a machine-readable format to be able to transmit it to another controller - should not be subject to a derogation, as it appears that this right is not applicable in the archiving context; and
- the ECB should seek support from their data protection officer before taking any decision to derogate from individuals' data protection rights.

4.2.3.
Processing employees' personal data

In 2022, Eurojust, the EU Agency for Criminal Justice Cooperation, sought our advice concerning the data protection implications of a new activity-recording tool to record the amount of time dedicated to various activities laid down in the Annual Work Plan by human resources to conduct activities more efficiently. This tool would imply the processing of the personal data of EUIs' employees.

Whilst the activity-recording tool may greatly benefit Eurojust, we expressed our scepticism towards the data processing operations which will be performed when the tool is deployed.

In our Opinion, we recommended that an executive decision, stating the exact terms of the processing operation, is included by Eurojust to complement Eurojust's Financial Regulation. This would include the purpose of processing; the criteria to determine the controller; the type of data subjected to processing; the purpose for which this data is processed; as well as several other measures necessary to guarantee lawful and fair processing.

Furthermore, we strongly advised the institution to double-check if the specificity of the activities and the size of the Units allow for the singling out of individuals. If this turns out to be the case, we advised that Eurojust adapts the information provided to individuals accordingly. Finally, we expressed our view that the legal framework in the contract entered between Eurojust, the processor and the sub-processor, should be updated.

4.2.4.
Data protection and competition law

In May 2022, we also issued a Supervisory Opinion pertaining to the processing of personal data in the context of competition law investigations, highlighting that Regulation (EU) 2018/1725 and EU competition law rules should be applied in a manner that is mutually compatible and enables them to be applied consistently.

4.3.
Conducting data protection audits

Audits are one of the tools we use to verify how data protection is applied in practice in EUIs. During an audit, we are able to verify compliance on the spot, and make recommendations when identifying areas for improvement. We sometimes share our findings publicly to promote public awareness of the risks, rules, safeguards and rights related to the processing of individuals' data.

In 2022, we conducted a total of 6 audits concerning:

- Europol - the EU Agency for Law Enforcement Cooperation;
- Frontex - the European Border and Coast Guard Agency;

- three large-scale information systems operated centrally by eu-LISA: the Visa Information System, the Schengen Information System II and Eurodac;
- e-recruitment procedures at ESMA - the European Securities and Markets Authority;
- the CdT - the Translation Centre for EUIs.

Due to the improved COVID-19 situation, we were able to conduct five of our audits in-person - known as on-the-spot audits, and only one audit was conducted remotely.

Two of our on-the-spot audits this year concerned Europol and Frontex on their data protection activities (see section 4.7). We also carried out three on-the-spot audits at eu-LISA, where we checked data protection compliance when using large-scale information systems, specifically the Visa Information System, the Schengen Information System II, which are systems used in the EU for border management, and Eurodac, the EU's fingerprint database for identifying asylum seekers and irregular migrants (see section 3.1).

4.3.1.
E-recruitment procedures

Our only remotely-conducted audit involved the processing of personal data in the context of recruitment, specifically when carrying out online assessments with remote invigilation adopted by a number of EUIs to adapt to the new circumstances of the COVID-19 pandemic.

Upon completing our audit on EUIs' e-recruitment processes, we recommended to assess whether practicing e-recruitment procedures is necessary post-COVID-19, whether a data protection impact assessment is required to assess the impact on individuals' personal data in this context; and to reconsider transfers of personal data when using a contractor located outside the EU/EEA to carry out the e-recruitment process.

We are currently assessing how the audited EUIs responded to these recommendations. By ensuring that our guidance is applied in this area, we aim to protect individuals.

4.3.2.
Schengen: privacy and freedom of movement

As part of our auditing work, and as the supervisory authority of certain EU's large-scale IT systems, we contributed, as an observer, to the Schengen Evaluation and Monitoring Mechanism (SCHEVAL) in the area of data protection.

SCHEVAL is a peer evaluation exercise assessing whether the rights and obligations related to Schengen (Schengen evaluations) are correctly applied by its members, which includes most EU Member States and several non-EU countries, and aims to enhance the freedom of movement for millions of individuals.

In 2022, we participated in four SCHEVAL missions in Luxembourg, Spain, Iceland and Denmark. In particular, we contributed to assessing the role and powers of national data protection authorities (DPAs), as well as the data protection rules, including transparency and security, applied to the Visa Information System and Schengen information System databases, and pushed for public awareness and cooperation amongst DPAs.

Our participation in SCHEVAL is one of the opportunities we have to constructively cooperate in the work of EU Member States' DPAs, and therefore ensure that data protection law is applied in a consistent and coherent way across EU.

4.4.
Handling complaints

Whilst we dedicate a large part of our resources to provide EUIs with timely advice on their activities impacting individuals' privacy and personal data, we also investigate complaints submitted by individuals who believe their data protection rights have not been respected by EUIs.

It is our duty to ensure that EUIs lead by example on data protection matters, and that they are held accountable if they fail to comply with data protection laws. In doing so, we help protect individuals' fundamental rights and enable them to take ownership of their personal data.

In 2022, we received 367 complaints; that's 47 more complaints than in 2021. Out of the 367 complaints handled, 65 were admissible and 302 were inadmissible. A complaint may be inadmissible, and therefore cannot be addressed by us, if, for instance, they are against private entities, national authorities and/or international organisations. During the year, the EDPS handled and finalised 47 complaint cases.

In 2022, we issued our first complaint decision that implemented the Schrems II judgment of the CJEU.

The complaint was lodged by 6 members of the European Parliament (EP) and concerned alleged infringements relating to information to be given to individuals and transfers or personal data to the United States of America (USA), in relation to an EP's website that offered COVID-19 testing to its staff members.

Following an extensive investigation of the complaint, we found a number of infringements, in particular, the EP's failure to fulfil its responsibilities as controller, its failure to use a processor that provides sufficient guarantees to implement appropriate technical and organisational measures, and its failure to comply with the principles of transparency and accountability, and uphold individuals' right to information and access to their data.

Furthermore, we found that the EP should not have relied on standard contractual clauses without having demonstrated that the personal data transferred to the USA were given an essentially equivalent level of protection.

In addition, we concluded that the EP used a tracking cookie without properly informing individuals. We decided to issue a reprimand to the EP for its infringements of Regulation (EU) 2018/1725, as well as an EDPS Order to update its data protection notices on the concerned website, in order to provide all relevant information relating to the processing of personal data. In determining the corrective powers to use, we took into account the possibly large number of individuals affected by the aforementioned infringements and the impact these had on their fundamental rights and freedoms, as well as the processing's duration.

In 2022, we also handled a complaint concerning an alleged infringement of Regulation (EU) 2018/1725 in the handling of a public access to documents request (ATD).

According to the complainant, the EUI disclosed their personal data to a third party when it gave access to un-redacted documents when responding to an ATD. The person that had made the ATD informed the controller about the possible personal data breach, but the EUI did not report the breach to the EDPS in a timely manner, nor did it inform the complainant about the breach, as it failed to detect the incident as a breach of Regulation (EU) 2018/1725.

We found that the EUI, as a consequence of its failure to identify and immediately react to the data breach, had indeed failed to notify the breach to us within the deadline prescribed by Regulation (EU) 2018/1725, and failed to communicate the data breach to the complainant. We decided to reprimand the EUI for these infringements.

Zoom in on our complaint procedures

The data protection law for EUIs, Regulation (EU) 2018/1725, states that the EDPS must handle complaints and investigate the subject matter of the complaint, to the extent that is appropriate. To ensure that we handle complaints in an efficient and relevant way, we have reviewed this year our rules of procedure and added the requirement that complainants should, in principle, lodge a complaint within two years after becoming aware of the facts.

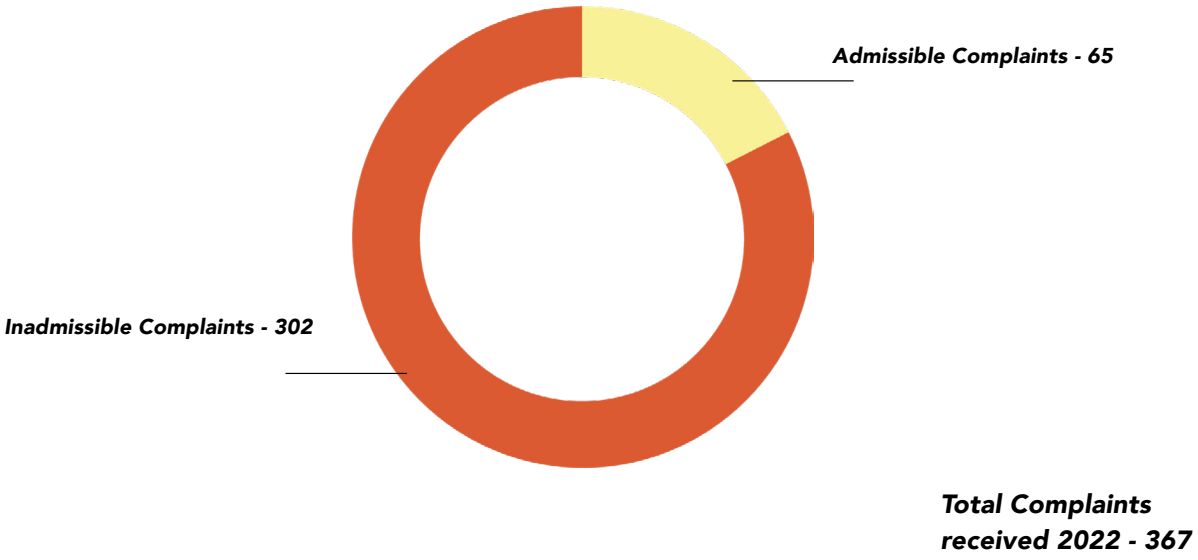
Our main reasons for deciding not to handle older cases are threefold. Firstly, for reasons of accuracy. Cases where the facts occurred a long time ago are always more complicated to investigate. Fact-finding becomes difficult, for example, due to organisational or structural changes, such as relevant employees retiring or leaving the EUI concerned. As such, the likelihood of establishing that an infringement has occurred is much lower.

Secondly, for reasons of legal certainty. Handling older cases may mean that we need to continue analysing facts under the previous data protection regulation applicable to EUIs, Regulation (EC) 45/2001, which is no longer in force.

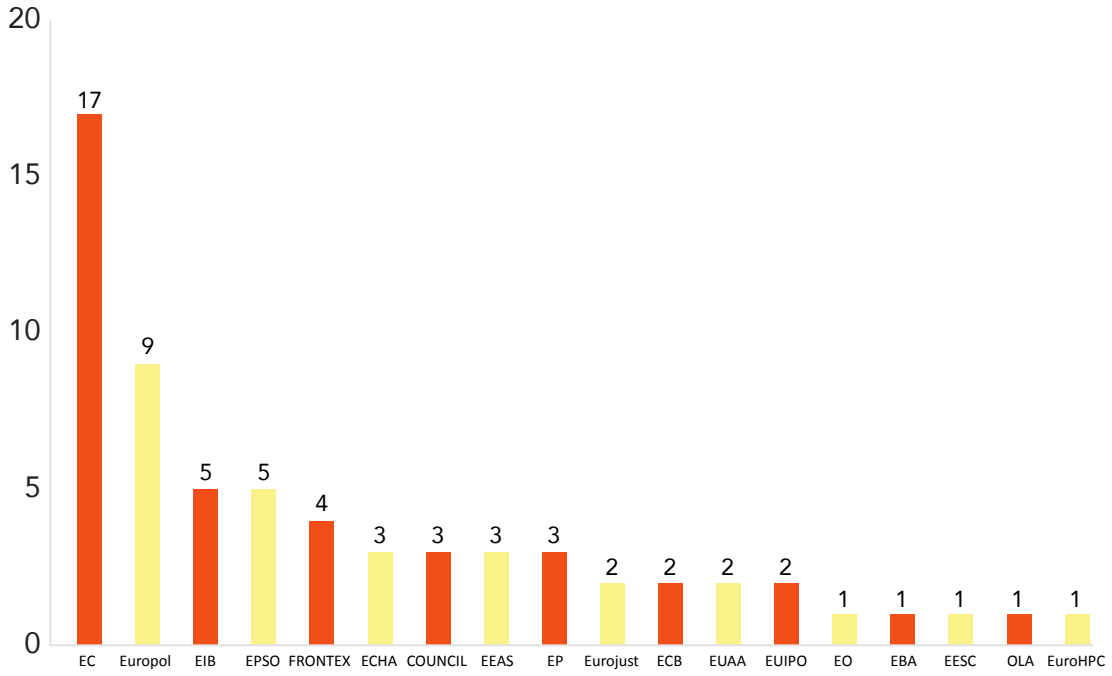
Thirdly, for reasons of good administration. Older complaints often mean that the current impact on the individual is lower. This could be because they are no longer employed by the EUI in question or simply because of the passing of time. We have therefore decided to concentrate our efforts on handling more recent cases where the current impact on individuals is higher and our decisions will have a greater effect.

In exceptional and duly motivated cases, we can nevertheless decide to investigate complaints that are lodged outside of the deadline if, for example, there were legitimate reasons for the complainant not to act in time or if the alleged infringements are serious.

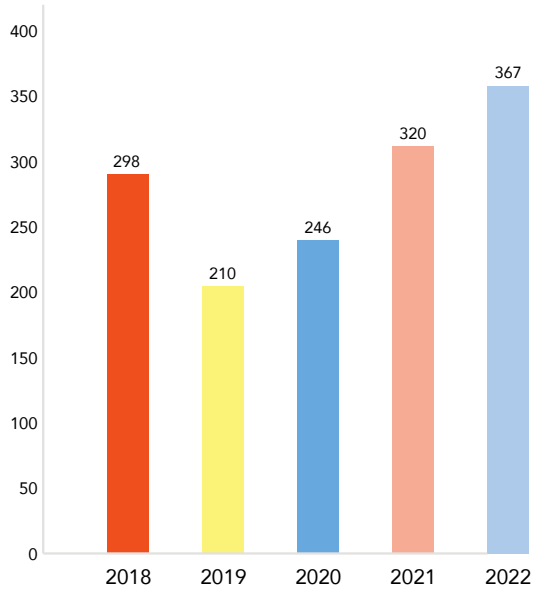
Number of complaints received per institution



Total Complaints received 2022 - 367



Admissible complaints per institution ***Grand Total 65***



Statistics of complaints received

1

EDPS Order under 58.2(e) of Regulation (EU) 2018/1725

4

EDPS Reprimands under under 58.2(b) of Regulation (EU) 2018/1725

4.5.
International data transfers

As the data protection authority of EUIs, we have the power to open an investigation when we have a strong suspicion that an EUI may have breached EU data protection law. By opening an investigation, we aim to check whether an infringement of the applicable data protection rules, in particular the Regulation (EU) 2018/1725, has occurred and to establish its circumstances.

The topic of international transfers - when personal data is transferred to countries or entities outside the EU or European Economic Area (EEA) - has garnered our attention increasingly over the last few years, demanding us to mobilise a significant percentage of our resources into tackling and monitoring related issues. This topic is particularly relevant given EUIs', including the EDPS, reliance on products and services from entities based outside the EU/EEA.

Our main goal in this area is to ensure that there is an essentially equivalent level of protection of individuals' personal data outside the EU/EEA as guaranteed in the EU/EEA. Pursuing this objective, we have developed strategic advice for EUIs, opened investigations and used our corrective or authorisation powers when necessary.

In particular, our investigations in 2022 focused on transfers of personal data to non-EU/EEA countries, specifically looking at EUIs' contracts with private entities, in particular large ICT providers. We also looked at arrangements between EUIs and non-EU/EEA countries or public bodies, or international organisations.

Aiming to lead by example in this area, we are working towards using alternative products and services that are based in the EU/EEA, and encouraging EUIs to consider the use of such EU/EEA-based products and services.

4.5.1.
Ongoing investigations following the Schrems II judgment

Following the 2020 Schrems II Judgment of the Court of Justice of the European Union, reaffirming the importance of maintaining a high level of protection of personal data transferred from the EU to non-EU/EEA countries, we issued a strategic document aiming to monitor EUIs' compliance with the judgement.

Upon executing the EDPS' Schrems II strategy, we found that the levels of awareness and compliance with EU data protection law amongst EUIs when carrying out transfers of personal data outside the EU/EEA appeared to be relatively low. However, since the EDPS' 2020 Order to all EUIs to carry out a transfer mapping exercise, and further guidance, the overall level of awareness and compliance in this area has progressed. Nevertheless, there is a need for further improvement, especially when it comes to implementing measures that will, in addition to contractual measures, mitigate the risks arising from non-EU/EEA legislation.

As part of our Schrems II strategy, we decided to focus our investigative activities on EUIs' use of cloud-based services. The use of cloud-based services frequently raises questions related to the role of the providers and data transfers. These are areas where critical compliance issues with Regulation (EU) 2018/1725 and Schrems II judgment can occur.

The investigations that we are carrying out in this area are part of a continuous cooperation between the EDPS and the EUIs to ensure a high level of protection of the fundamental rights to protection of personal data and to privacy. We also aim to highlight the need to properly assess the necessity and proportionality of the personal data processing in cloud services, including looking into alternative solutions or providers that imply less interference with fundamental rights.

In May 2021, we launched two EDPS investigations in particular. One concerns all EUIs, covering transfers of personal data when using cloud services provided by Microsoft and Amazon Web Services under Cloud II contracts. The other investigation concerns the European Commission's use of Microsoft Office 365. The two investigations were pursued in 2022 and will continue in 2023. They are complex - both in terms of substance and procedure - and require significant investment of resources.

4.5.2.
A pre-investigation: international data transfers

In 2022, we pre-investigated the use of the cloud service Trello, a US-based company, by an EUI.

During our pre-investigation, we requested information that could prove EUIs' compliance with the requirements set out in Chapter V of Regulation (EU) 2018/1725 concerning transfers of personal data outside EU/EEA countries. These requirements include, for example, ensuring that the level of protection of individuals guaranteed by that Regulation is not undermined when their personal data is transferred outside the EU/EEA. We also asked for information on whether the processing of individuals' personal data was processed in a secure way. This information was necessary to determine whether to open a formal investigation.

In the course of our pre-investigation, we were informed by the EUI in question that it had not given its approval for the use of Trello by its employees. The EUI also informed us that it would carry out its own IT assessment of Trello and that it would issue a recommendation to its departments not to use this tool.

4.5.3.
A complete investigation: reprimanding Frontex

On 1 April 2022, we reprimanded the European Border and Coast Guard Agency (Frontex) for a breach of Regulation (EU) 2018/1725.

We issued this decision following an investigation on Frontex's move to a hybrid cloud consisting of Microsoft Office 365, Amazon Web Services (AWS) and Microsoft Azure, following an investigation initiated in June 2020.

Our investigation looked at Frontex's compliance with Regulation (EU) 2018/1725, taking into account EDPS Guidelines on the use of cloud computing services issued in 2018, which outline the approach that EUIs should take to ensure the protection of personal data when considering the option of using cloud computing services for their IT systems.

We found that Frontex moved to the cloud without a timely, exhaustive assessment of the data protection risks and without the identification of appropriate mitigating measures or relevant safeguards for processing.

Frontex also failed to demonstrate the necessity of the planned cloud services, as it has not shown that the chosen solution, Microsoft 365, was the outcome of a thorough process whereby the existence of data protection compliant, alternative products and services meeting Frontex's specific needs were assessed.

In addition, Frontex failed to demonstrate that it limited Microsoft's collection of personal data to what is necessary, based on an identified legal basis and established purposes. Therefore breaching the accountability principle, as well as its obligations as a controller and the requirements of data protection by design and by default - which are principles to apply throughout the use and development of technologies, to ensure that these are privacy compliant.

On top of the reprimand, we ordered Frontex to review its Data Protection Impact Assessment and the Record of Processing activities relating to the processing of personal data in cloud services.

We stressed that it is the controller's responsibility towards competent authority and towards individuals whose data is processed to clearly identify the activities requiring the processing of personal data and to assess the impact on individuals' fundamental rights. This analysis must be carried out properly before taking any decisions to process personal data.

4.5.4.
Tools to transfer personal data: contractual clauses and administrative arrangements

We are regularly requested to authorise transfer tools, notably contractual clauses and administrative arrangements, which are one of the ways EUIs are able to transfer personal data to non-EU/EEA countries or international organisations, whilst still ensuring that individuals' information is adequately protected. In 2022, we granted authorisations both for contractual clauses and administrative arrangements.

When granting authorisations to EUIs, we highlighted that transfers of personal data may only occur if done in compliance with EU law. This implies that the protection of individuals' data is essentially equivalent as guaranteed in the EU/EEA.

We also provide suggestions on how to carry out transfer impact assessments which help identify necessary effective supplementary measures that should be put in place in the context of transfers.

With our guidance, we always emphasise that if no essentially equivalent level of protection is ensured, notably with effective supplementary measures, the transfers will not be allowed. We also underscored the importance for EUIs to remain in control of the whole chain of processing and that EU law is respected, in particular in case of transfers.

This work is part of our strategy to ensure that ongoing and future international transfers comply with the EU Charter of Fundamental Rights, applicable EU data protection legislation and the Schrems II judgement of the CJEU.

Data transfers in the field of air traffic management

In December 2022, the EDPS authorised an Administrative Arrangement between the Single European Sky ATM Research 3 Joint Undertaking (SESAR) and the European Organisation for the Safety of Air Navigation (Eurocontrol). An Administrative Arrangement maps out the procedures, safeguarding measures, and other relevant measures to ensure that transfers of personal data outside the EU or the EEA or to international organisations are carried out whilst ensuring an essentially equivalent level of protection of individuals' personal data to that guaranteed inside the EU and the EEA.

SESAR is a European public-private partnership that aims to help Europe's aviation infrastructure and related technologies to be better prepared for future demands in this area. Eurocontrol is a member of SESAR. SESAR staff will be moving to Eurocontrol's premises and will benefit from Eurocontrol's logistics and infrastructure support, such as IT resources, access control services, etc., which involve transfers of personal data.

Upon assessing the Administrative Arrangement in question, we commented on a number of recurring issues that come up in cases involving transfers to international organisations. In particular, we recommended that an independent oversight mechanism, functionally autonomous within Eurocontrol, is put in place. This independent oversight must also have the authority to issue decisions binding Eurocontrol. We also advised that a mechanism that enables individuals to obtain effective redress and remedies free of charge, including compensatory measures, is put in place as well.

As a way to resolve some of these issues, Eurocontrol aims to modernise its data protection framework by the end of 2023. In the meantime, Eurocontrol and SESAR will rely on the International Court of Arbitration of the International Chamber of Commerce to fulfil the role of oversight and judicial redress temporarily. On that basis, we authorised the Administrative Arrangement temporarily, effective until 30 June 2024.

Communication tools and data transfers

In October 2022, we issued a Decision temporarily and conditionally authorising the use of contractual clauses between the Court of Justice of the EU (the Court) and Cisco Systems Inc. US, which provides online communication tools. The Court's use of this tool and related services results in transfers of personal data of the Court's users.

This Decision is a follow-up to an earlier Decision from August 2021, in which we imposed 11 conditions that the Court had to follow. Upon verification, we concluded that, while areas of partial or non-compliance remained, the Court had taken steps towards complying with recommendations.

In our 2022 Decision, we reiterated the importance of taking into account the impact of privileges and immunities protecting EUIs' data in the context of transfers of personal data. As a result of the specific legal context of EUIs, we also underlined the need to adapt, and seek the EDPS' authorisation for the standard data protection clauses for transferring personal data adopted under the General Data Protection Regulation to the obligations under Regulation (EU) 2018/1725 applicable to EUIs.

Our 2022 Decision authorises the use of contractual clauses until 31 October 2024 and the Court must ensure compliance by 1 March 2024. We will verify this compliance gradually through reports submitted by the Court demonstrating actions taken to achieve this.

4.5.5.
The use of non-EU products and services: towards EU institutions' compliance

In addition to our ongoing investigations into EUIs' use of products and cloud services from entities based outside the EU/EEA, in particular the European Commission's use of Microsoft Office 365 (see 4.5.1), we have also issued guidelines and policies, as well as provided training sessions to EUIs.

These efforts aim to raise EUIs' awareness of the risks posed by using tools or conducting data processing activities that imply transfers of data outside the EU/EEA. We also aim to raise EUIs' awareness of the contractual safeguards and other measures to put in place to ensure that individuals' personal data is protected in an essentially equivalent way outside of the EU/EEA.

Our guidance this year focused on ensuring that EUIs use services and products based outside the EU/EEA only when strictly necessary, hence encouraging them to seek alternatives that would not involve international transfers. We also advised EUIs on how to renegotiate their contracts with providers to ensure that EUIs have full control over the processing of data, and how to use transfer tools provided in Regulation (EU) 2018/1725, such as standard contractual clauses and administrative arrangements properly to protect individuals.

Centralising our advice and recommendations provided to EUIs in this area, we published in April 2022 a short factsheet, in which we stressed that EUIs must ensure that the whole chain of processing by them and on their behalf meets the requirements of Regulation (EU) 2018/1725 to effectively protect the rights of individuals. When EUIs procure tools with which they process personal data or when they engage the services of processors to process personal data on their behalf, they bear legal obligations as the controller of that processing. In line with the principles of data protection by design and by default, EUIs must also consider the most data protection and privacy-friendly solutions.

Given the importance of this topic, we also actively participated in the ongoing 2022 Coordinated Enforcement Action (CEF) of the European Data Protection Board. The coordinated action, which started on 15 February 2022, includes a series of actions taken by 22 data protection authorities of the EU, including the EDPS, to ensure that public bodies in the EU and EUIs comply with EU data protection law when they use cloud-based services. The first results of the coordinated action were gathered in the EDPB Report on the 2022 Coordinated Enforcement Action (see Chapter 7).

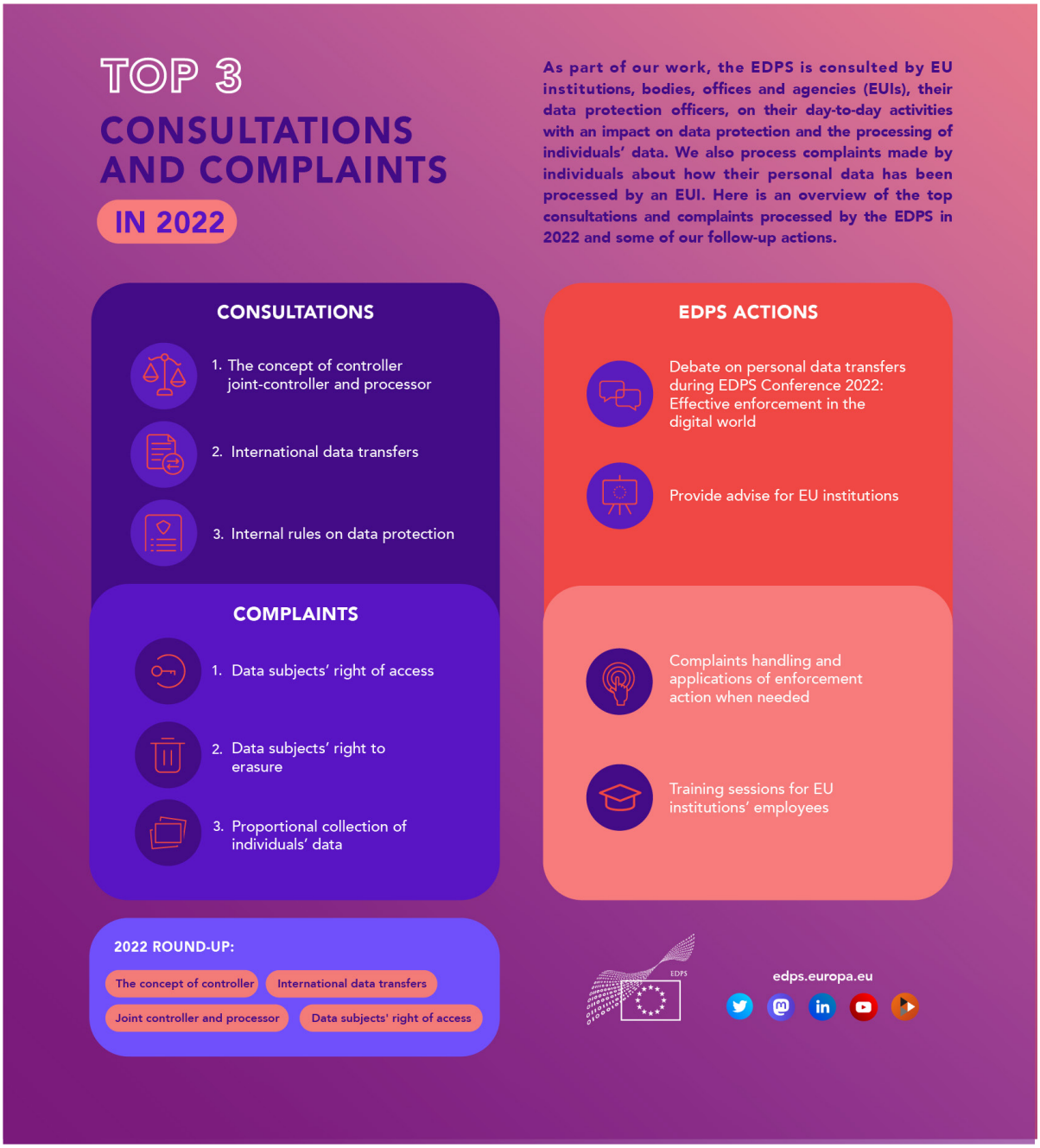
4.5.6.
Seeking alternatives: using EU products and services

Being an independent supervisory authority does not only consist of monitoring how EUIs process personal data, but also means holding our organisation, the EDPS, accountable too.

Rallying all competencies together as an organisation, we analysed the data protection opportunities and challenges relating to the procurement of Software-as-a-Service (SaaS) and other hosting services from an EU-based provider, between November 2021 and April 2022.

We identified the data protection requirements that needed to be considered, building criteria for selecting EU-based providers before launching any procurement procedures. In addition, we listed the data protection guarantees that the chosen provider would have to comply with. This included ensuring that processing only takes place in EU/EEA countries and that extra-territorial legislation of countries outside the EU/EEA does not apply. Furthermore, we established which technical, organisational and security measures must be put in place by the EDPS and the provider.

Leading by example as an organisation, by using alternative tools that respect individuals' privacy, is a solid step towards making data protection by design and by default a reality. By demonstrating that this is possible, we, in turn, encourage other EUIs to follow this path. This is why we worked on procedures and negotiated the procurement of EU-based SaaS and other hosting services that EUIs can also benefit from. As such, we concluded and will lead an inter-institutional contract for the Nextcloud software hosted by TAS France. The services under this contract will be rolled out at the beginning of 2023 as a pilot project.



4.6.
Cooperating with EU institutions and their data protection officers

Building and maintaining a strong cooperation with EUIs, their employees and data protection officers allows us to work hand-in-hand to protect individuals' personal data, according to EU data protection law.

4.6.1.
The network of data protection officers

To help bridge the gap between data protection law, in particular Regulation (EU) 2018/1725, and its practical application, we continuously foster collaboration with 70 data protection officers (DPOs) of the EUIs, which compose the network of DPOs, established over 18 years ago.

The role of DPOs has become increasingly important over the years, especially since the adoption of the General Data Protection Regulation and Regulation (EU) 2018/1765. With their knowledge of data protection, their EU institution and its activities, DPOs are able to provide independent, tailored advice and measures on data protection matters, whilst meeting the needs of their organisation.

As part of our collaboration with DPOs, two meetings are held each year. The objectives of these meetings are to take stock of the work done in the data protection field, and to approach challenges that have or may arise in a solution-focused way to achieve compliance with data protection law, and therefore protect individuals' data. We can then provide support accordingly.

The two meetings held in 2022 were especially anticipated as it was the first time since 2019 that we were able to meet in person with the network of DPOs due to the COVID-19 pandemic. A group of DPOs, the DPO Support Group, actively contribute to their organisation, by suggesting topics for the agenda, preparing case studies and co-facilitating workshops, for example.

Amongst the multitude of topics discussed, particular focus was put on the use of social media by EUIs, personal data breaches, handling individuals' requests to access their personal data, and other practical guidance based on issues either encountered by data protection officers, or issues that have been subject to case law. To maximise their interactivity, workshops, activities and presentations were organised to facilitate discussions amongst DPOs, and between DPOs and the EDPS.

These exchanges provide helpful feedback from DPOs, which, in turn, contribute to informing our work when producing guidelines, organising training sessions and providing advice.

4.6.2.
Delivering training

Another way we collaborate with DPOs and their EUIs is through the organisation of regular training sessions at the European School of Administration (EUSA).

We also organise on-demand training sessions which are tailored to the EUIs' core activities and the related data protection challenges they may encounter. Participants of these training sessions are EUI's members of staff, who may have a varied understanding of data protection, and their DPO(s).

A new, easily accessible data protection learning plan

To increase awareness on the topic of data protection even more and make it easier to comprehend, we launched in March 2022, a Learning and Development Plan (Learning Plan) for EUIs' employees including a series of online training courses and recorded online talks prepared with EUSA.

The Learning Plan starts with an introduction to the data protection rules applicable to the EUIs – Regulation (EU) 2018/1725 (or EUDPR), with a course titled "EDPS course on Data Protection - EUDPR fast-track training course for practical application in your daily tasks".

The advanced level of the Learning Plan is composed of various online talks, presentations, case studies. They provide detailed explanations on data protection rules and principles that apply when processing individuals' personal data in different circumstances often encountered by EUIs and their staff when planning events, carrying out procurement procedures and other outsourcing activities, for example when using social media. It also focuses on the data protection implications of using ICT tools, on personal data breaches, and on transfers of personal data, as well as many other topics.

With this Learning Plan, EUIs' staff can learn at their own pace, as these courses can be accessed at any time via the EU institutions' learning platform, EU Learn.

Training sessions: a way to ensure data protection compliance

Additionally, we provided 22 training sessions to EUI staff, as well as externally, addressing for example students or judges.

Some training sessions covered the enabling and restricting of individuals' data protection rights, such as their rights to access, rectification, erasure, in the context of EUIs' selection procedures and other administrative enquiries. In other training sessions, the topic of data protection and audits was discussed. In particular, how to apply the principles of data minimisation and purpose limitation - to process only data that is strictly necessary for the objectives pursued - when audits are conducted by the EDPS.

In another series of training sessions, EUIs' staff learned about common issues raised in recent DPA and judicial cases concerning social media. Issues discussed included the role of the social media platform provider, the reuse and sharing of data, data security, as well as pervasive tracking and profiling. Training sessions were also organised on international data transfers (outside the EU/EEA) and the use of cloud services by EUIs.

This work is aligned with our greater efforts to provide EUIs with appropriate tools to enable them to effectively safeguard individuals' personal data, when conducting their daily activities. It is crucial for EUI members of staff to acquire sufficient knowledge of data protection and be aware of their obligations under EU data protection law.

4.7.
Supervising the Area of Freedom, Security and Justice

As part of our work, we also supervise the data processing operations of the following bodies 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).

These bodies 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 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 Agencies and Bodies, 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 in charge of the supervision of Europol, Eurojust and EPPO. This therefore allows us to ensure 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. More details on this work can be found in Chapter 7: Achieving Together.

In 2022, our supervisory activities in the AFSJ focused on the following issues:

- Monitoring the application of the principle of data protection by design in new IT systems and processes, where we identified a lack of systematic approach in this area. We also identified some deficiencies in the data protection risk assessment process at Europol which, in turn, also affected Europol's ability to plan effective mitigation measures.

- Paying specific attention to the efficient application of individuals' data protection rights, in particular in the context of our investigations of complaints against Europol.

- Developing and strengthening cooperation with EU/EEA's data protection authorities in order to develop joint supervision, both through our participation to the Coordinated Supervision Committee and specific joint supervisory activities together with these authorities. This resulted in particular in the signing of a Working Arrangement with the Portuguese DPA in the context of EPPO. We also actively participated in the drafting of Article 37 Law Enforcement Directive Guidelines in the context of the EDPB (see Chapter 7).

- Supervising Frontex, which has revealed that the vague or excessively complex wording of the Agency's Regulation is creating uncertainties regarding the exact scope of their tasks, opening the door to different interpretations, in particular in the context of personal data collection for purposes of identifying suspects of cross-border crime, of risk analysis, or EUROSUR - the European Border Surveillance System.

- Following-up closely the correct application of data protection safeguards by Eurojust in the context of the development of the war crime module; an activity which will continue in 2023.

4.7.1.
Accountability and data protection by design

In 2022, we focused on the methodology and processes put in place by AFSJ Agencies and Bodies to uphold the principle of data protection by design.

Data protection by design aims to build data protection and privacy into the design of processing operations, information systems, and the development of technologies, for example, in order to comply with data protection obligations and laws. Organisations are required to take into account the protection of the rights of individuals, both before and during their processing activities, by putting in place the appropriate technical and organisational measures to ensure that they fulfil their data protection obligations. This requires to have appropriate methodologies and processes in place.

To achieve data protection by design practically, AFSJ Agencies' and Bodies' data controllers are obliged to draft Data Protection Impact Assessments (DPIAs) and submit them for prior consultation to us when the processing involves high risks for individuals. This also contributes to fostering accountability. It remains crucial that, through DPIAs and prior consultation tools, the most risky processing operations are properly assessed, given the already sensitive nature of the police and judicial cooperation and border management fields.

Methods and processes applied to design new systems

This year, we advised several AFSJ Agencies and Bodies on how to achieve data protection compliance during the development of their software for new IT systems. We were able to provide advice by assessing their compliance with envisaged data processing operations, analysing in particular the risks that these may pose to individuals and the mitigating safeguards planned. We explored how AFSJ Agencies and Bodies can integrate the principles of transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability to each step of each software development and testing process.

For example, in March 2022, we opened an enquiry into Europol's New Environment for Operations (NEO), because of our concerns regarding Europol's fragmented approach, impacting its compliance with data protection by design, and its keeping of records of processing activities. To carry out our enquiry, we collected information on the IT processes used in the context of NEO, to develop and test new NEO components. This allows us to look into the application of data protection by design in more detail to check if this is done effectively.

We also provided our support to Eurojust in its move to a more effective and efficient Case Management System (CMS). For the development of the CMS, Eurojust chose to use a contractor for a study and market research to see if there are any existing solutions that would meet the Agency's needs. We therefore looked at the data protection by design aspects of the development of this new CMS. Given that a contractor is being used, applying measures upholding these data protection principles is different and required us to examine the data protection elements defined by the contractor, to ensure compliance.

Similarly, we carried out an audit at Frontex. We inspected two aspects in particular. We first examined the IT security surrounding the activities and production of reports for the screenings, debriefings and intelligence reports, including data flows, data repositories, external data exchanges, state-of-the-art technical infrastructure. We then looked at Frontex's new IT systems, which were being developed by both external contractors, as well as internally. This required us to both look into the contractors' obligation regarding data protection by design and Frontex's way of including data protection by design into their internal development processes.

Verifying whether data protection by design is being applied in Europol's, Eurojust's and Frontex's activities will continue throughout 2023.

4.7.2.
Advising on data protection obligations

In 2022, we issued 9 Supervisory Opinions. That's 7 concerning Europol, 1 concerning EPPO and 1 concerning Eurojust. All of these Supervisory Opinions were issued on measures and operations envisaged by AFSJ Agencies and Bodies that may affect individuals' personal data.

Europol

Some of the Supervisory Opinions we issued concerning Europol related to its New Environment for Operations. For example, we issued a Supervisory Opinion on SIREN, a read-only analytical and visualisation tool under the umbrella of the Visualisation and Analysis Toolbox (VAT). To ensure full compliance with data protection law, we recommended that Europol ensures that the processing of personal data is limited to what is necessary, otherwise known as purpose limitation. We also advised that mechanisms and measures are put in place to mitigate the risks of errors linked to the use of SIREN's analytical capabilities, by conducting regular checks and updating IT log-ins and accesses.

We also looked at Europol's data refinery area, including tools for data transformation, triaging, and visualisation. We considered that Europol had insufficiently described the processing operations and the specific risks stemming from the data refinery area. Consequently, we were unable to make concrete proposals on Europol's compliance in this area. Nevertheless, we identified some of the high risks that may affect individuals and their personal data, which we recommended Europol to address promptly.

We issued other Supervisory Opinions on a variety of topics.

For example, we commented on a number of Europol's IT systems. Specifically concerning:

- Europol's use of the Schengen Information System (SIS II) to process individuals' fingerprints;
- the participation of Europol in the pilot project for a European Police Record System (EPRIS) aiming to automate the searching of police records indexes of its participating EU Member States;
- QUEST+ - an interface used to exchange personal data between EU Member States' systems and the Europol Information System;
- the development of PERCI, the European platform for taking down illegal content online.

For most of these IT systems, we found that Europol had not identified all of the specific risks that these systems posed to individuals' privacy and data protection rights. In our view, this issue resulted from an incorrect, or incomplete, data protection impact assessment, which, in turn, also affected Europol's ability to plan effective mitigation measures, especially in light of the sensitive data processed, such as data related to health, religious belief, sexual orientation, in the event of a data breach for example. To this end, we issued 8 recommendations tending to improve the internal data protection risk assessment process. Our recommendations were issued in a report following our Annual Inspection conducted in 2021.

Aside from addressing these recurrent issues, we also provided more specific recommendations on these IT Systems.

Regarding Europol's use of SIS II, we provided further recommendations on purpose limitation - to limit the collection of data for a specific purpose - on processes relating to access to information, and on data accuracy and data security.

Concerning QUEST+, we urged Europol to ensure that this system does not allow searches of individuals' personal data that have not been through the full extraction process, to uphold the principles of data minimisation and data accuracy. The data extraction process involves checking for personal data related to crime within a large volume of data that has been collected and to discard personal data that is not relevant.

Addressing the use of PERCI, we provided more tailored recommendations relating to transfers of personal data from outside the EU/EEA, on cloud-computing security, for example.

EPPO

In July 2022, we were consulted by EPPO concerning its newly planned IT environment for operational analysis. This new environment was deemed necessary because EPPO's case management system (CMS) is not equipped with tools to analyse large files, such as voluminous financial documentation.

As such, EPPO sought our advice to be able to use the Case Analysis Tool Environment (CATE), as a separate and secured environment that allows them to import data from the CMS, conduct the analysis and export the results back to the case file. We therefore made recommendations on this tool, addressing issues related to the categorisation of individuals' personal data, how long this data is to be retained, and the development of a policy when using these tools to ensure that individuals' personal data is protected.

Eurojust

Eurojust consulted us on two occasions for the setup of their new automated data management and storage facility, CICED - Core International Crimes Evidence Database. This new project is essential to Eurojust in its role as a European hub for storing, preserving and analysing evidence of genocide, crimes against humanity and war crimes.

As a supervisory authority, our contribution here was particularly important to ensure that Eurojust can fulfil its role of protecting individuals from crime by seeking justice, whilst ensuring that individuals' personal data is protected, particularly when dealing with sensitive evidence. We therefore touched base with Eurojust at every stage of CICED's development, from transmitting big files from national authorities to Eurojust. The development of CICED is ongoing, and will continue to be a focus of our work throughout 2023.

4.7.3.
Police cooperation

Europol's processing of large datasets

In 2022, we finalised our investigation on "Europol's big data challenge", initially launched in 2019. This resulted in the EDPS ordering Europol to erase data concerning individuals with no established link to criminal activity - known as Data Subject Categorisation, on 10 January 2022.

Our EDPS Order followed an EDPS Admonishment that we issued in September 2020 because Europol continued to store large volumes of data with no Data Subject Categorisation, which poses a risk to individuals' fundamental rights. While some measures have been put in place by Europol since then, Europol has not complied with our requests to define an appropriate data retention period to filter and to extract the personal data permitted for analysis under the Europol Regulation. This means that Europol was keeping this data for longer than necessary, contrary to the principles of data minimisation and storage limitation, enshrined in the Europol Regulation.

In light of the above, we decided to use our corrective powers, imposing a 6-month retention period to Europol to filter and to extract individuals' personal data. Datasets older than 6 months that have not undergone this Data Subject Categorisation must be erased. This means that Europol will no longer be permitted to retain data about people who have not been linked to a crime or a criminal activity for long periods with no set deadline. We have granted a 12-month period for Europol to comply with the Decision for the datasets already received before this decision was notified to Europol.

As such, throughout 2022, our efforts focused on making sure that Europol complied with the EDPS Order. One of the ways we checked this compliance is by reviewing Europol's quarterly reports evidencing the progress achieved regarding the erasure of datasets that were not compliant with the Europol Regulation. This continues to be a challenge, especially since Europol's Regulation was amended and entered into force in June 2022, legalising retroactively the possibility for Europol to process large data sets which may include individuals' personal data that has no link with criminal activity. In this context, we have asked Europol to provide updates on the application of the EDPS Order.

The impact of Europol's amended Regulation

The amendments to the Europol Regulation, Regulation (EU) 2022/991, that entered into force in June 2022, have shifted the balance between data protection and Europol's operational needs, as it expands considerably the Agency's mandate regarding exchanges of personal data with private parties, the use of artificial intelligence, and the processing of large datasets. We believe that these changes heighten the risks to individuals' personal data.

In particular, the amended Europol Regulation provides for a new legal basis for Europol to process large datasets which haven't undergone the categorisation process; these datasets were the subject of the EDPS Order.

One of these provisions, article 18a, allows Europol to retain personal data, including and excluding information linked to crime, for up to three years. Whilst the other provision, article 18 (6a), allows Europol to retain personal data, including and excluding information linked to crime, for the entire duration of an investigation, however long it may be. These rules would apply according to specific circumstances. The amended Europol Regulation mandates the Management Board to further specify the conditions of application of these articles, subject to prior formal consultation of the EDPS.

In this context, prior to the amended Regulation coming into force, we were informally consulted by Europol on draft texts. However, Europol's Management Board opted to adopt the Decision without prior formal consultation of the EDPS. Considering the aggravating risks these new processing activities pose to individuals, we decided to use, for the first time, our corrective power to refer a matter to the Commission, the Council and the European Parliament. There are a few reasons that brought us to making this decision. Aside from the substance of the problematic provisions, Europol infringed the EDPS powers and our decision-making agency by not consulting us formally on such significant matters, which is a legal requirement stemming from the Europol Regulation.

As a follow-up, Europol did consult us formally. In turn, we were able to issue a Supervisory Opinion, clarifying our interpretation of the scope of application of Article 18a of the amended Europol Regulation, which allows Europol to process datasets without an attributed data subject category for the purpose of supporting a specific ongoing criminal investigation upon request of a Member State, EPPO, Eurojust or a non-EU/EEA country for the whole duration of the investigation, and beyond, under specific circumstances.

We consider that Article 18a is a stand-alone provision which is meant to apply to specific cases, such as ongoing specific criminal investigations, that require the processing of large and complex datasets, for which Europol is better placed to detect cross-border links, such as the ones that prompted the creation of operational taskforces Fraternité, EMMA, LIMIT or Greenlight. These operational task forces are temporary, specialised teams of Europol experts and law enforcement officials from EU Member States that are brought together to work on specific operational tasks. The scope of Article 18a is thus not defined by the nature of the datasets received (with or without a Data Subject Classification) but rather by the need to support a specific ongoing criminal investigation at the request of the contributor.

Handling complaints to protect individuals' rights

In addition to providing advice to AFSJ Agencies and Bodies on how to comply with EU data protection law, we also addressed complaints made by individuals if they believe that their data protection rights have been infringed.

We also reviewed our procedures in this area in an effort to streamline our work, to improve our efficiency by increasing on-the-spot checks, scrutinising AFSJ Agencies' and Bodies' internal handling of individuals' data requests, and collaborating closely with EU Member States' data protection authorities when investigating complaints.

In 2022, we received 6 new complaints against Europol. Out of these 6 complaints, we issued 3 decisions, 2 of which resulted in using EDPS corrective powers, the remaining complaint is part of our ongoing work.

Concerning the first complaint for which we used our EDPS corrective powers, we found that Europol had breached its legal obligation to provide access to a complainant's personal data, without sufficient justification. In addition, Europol did not properly document the legal and factual reasons for this decision, thereby breaching its obligations under the Europol Regulation and the EU Charter of Fundamental Rights. Further, it transpired that Europol had not consulted the competent EU Member States' national authorities before issuing this decision.

Concerning the second complaint for which we also used our corrective powers, we found that Europol had violated the legal deadline laid down in the Europol Regulation which obliges the Agency to reply to individuals' access requests within three months.

For both of these complaints, we decided to admonish Europol for breaching several legal obligations. In one of them, we also ordered the Agency to provide access to the complainants with their data.

4.7.4.
Supervising data protection in EU border management

Increasing our scrutiny of Frontex

Over the last few years, Frontex - the EU Agency responsible for coordinating and developing European border management in line with the EU Charter of Fundamental Rights - has grown substantially, becoming one of the largest EU Agencies.

To match this evolution, we have doubled down on our support in supervising Frontex's activities that have an impact on data protection.

Processing of personal data in joint operations

One of Frontex's main tasks is to help EU Member States when they require technical and operational assistance at external borders, by coordinating and organising joint operations, which involve the collection of individuals' personal data.

We first conducted an operational visit at Frontex's headquarters, on 29 and 30 March 2022. The aim of the visit was to gain a better understanding of Frontex's activities and role in the context of joint operations.

Information gathered during our visit also contributed to the preparation of our audit, held in October 2022, in which we focused on whether the collection and further use of personal data for risks analysis and for purposes of identifying suspects of cross-border crime was compliant with data protection law, in particular in the context of Frontex's interviews with irregular migrants.

Frontex's rules on processing of personal data

In June 2022, we issued two Supervisory Opinions on two decisions adopted by the Management Board of Frontex on their rules for processing personal data.

The first Supervisory Opinion concerned Frontex's internal rules applicable to all of its personal data processing activities. The second Supervisory Opinion concerned Frontex's personal data processing activities related to the identification of suspects involved in cross-border crimes.

In these Opinions, we expressed two main concerns.

Firstly, the lack of a clear definition of key data protection elements in the Agency's internal rules, for example a lack of explanation on the specific purposes for which personal data about migrants and asylum seekers is collected, and on the categories of data collected for these purposes. We expressly highlighted that these elements are necessary to ensure that the data processing is foreseeable to individuals' concerned, according to the requirements of the EU Charter of Fundament Rights.

Secondly, we noted that several internal rules seemed to expand Frontex's role and tasks as a law enforcement authority which, under the Treaty on the Functioning of the EU, is the responsibility of another EU Agency. As such, we highlighted that Frontex's role in this area should be strictly limited to supporting the EU Agency and the EU Member States' authorities in charge of law enforcement tasks.

Transfers of personal data across external borders

We also provided advice in the context of transfers of personal data across external borders.

EUROSUR is a framework for information exchange and cooperation between EU Member States and Frontex to improve situational awareness and increase reaction capability at external borders. It is a multi-purpose system that aims to prevent, detect and combat illegal immigration and cross-border crime, and contributes to protecting migrants' lives.

Frontex submitted a request for authorisation of transfers to the Republic of Niger, in the context of a Working Arrangement establishing operational cooperation between Frontex and the Republic of Niger, as they plan to exchange personal data to counter irregular migration and cross-border organised crime. The Working Arrangement involved the transfer and exchange of personal data such as the exchange of identification numbers of aircraft which could in turn identify individuals, including

migrants and asylum seekers. We assessed whether this data would be afforded an equivalent level of protection outside the EU/EEA. We found that the working arrangement did not meet the strict conditions imposed by the Frontex Regulation on transfers of personal data to non-EU/EEA countries.

The transfer impact assessment conducted by Frontex revealed that while the Niger data protection law appears to offer a similar level of protection as in the EU, there is a risk that such law is not applied or complied with in practice. It also revealed that the identification numbers of aircraft, which could be used to identify passengers, potentially including migrants and asylum seekers, travelling on that aircraft may fall under the scope of repressive migration legislation. The transfer impact assessment referred in this context to a series of security-oriented legislative and policy measures undertaken by the Republic of Niger, resulting in reforms which have undermined the human rights of migrants. Therefore, we requested Frontex either to remove provisions for the exchange of data within EUROSUR; propose supplementary measures for this transfer; or demonstrate that problematic legislation will not be applied in practice to the transferred data.

Against this background, we visited the Agency's headquarters to understand better the personal data processing activities involved in EUROSUR. Following this visit, we are particularly concerned about the lack of clarity in the EBCG Regulation about the categories of personal data that can be processed and the scope of application of the data protection provisions to EUROSUR.

Digital borders: protecting the rights of people on the move

We continued to take on an active role within the Supervision Coordination Groups, which were established to coordinate the supervision of the EU's large-scale IT Systems, for example the Schengen Information System II (SIS II), or the Visa Information System (VIS).

In addition to reporting on audits carried out in SIS, VIS, we worked on a common audit reporting framework in the Supervision Coordination Group of Eurodac, the EU large-scale IT system contributing to the management of asylum applications by storing and processing migrants' and asylum seekers' fingerprints. Our work aims to streamline data protection inspections in this field.

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

Preparing for a new EU large-scale IT system

2022 saw ongoing preparations for the entry into force of a new EU large-scale IT system: the European Travel Information Authorisation System (ETIAS), created to identify security, irregular migration or high epidemic risks posed by visa-exempt visitors travelling to the Schengen Member States.

It is in this context that we contributed to the setting up of the ETIAS Fundamental Rights Guidance Board (EFRGB), which was formally established and held its first meeting in November 2022.

The EFRGB, of which the EDPS is a member, will assess, and issue recommendations, on the impact and risks that the processing of ETIAS applications has on individuals' fundamental rights, especially concerning the system of algorithmic profiling. Based on different factors, including our assessments, the EFRGB examines, in particular, the impact of ETIAS' operation on individuals' rights to privacy, personal data protection and risks to discriminatory practices.

We also advised that the EFRGB sets up a Working Group for ETIAS' Screening Board of applications of visa-exempt visitors travelling to Schengen Member States, and to set up a Working Group on ETIAS Risk Screening Operations, composed of Frontex, Europol and ETIAS National Units who are in charge of related processing of data.

Biometric data

The EU Agency for Operational Management of Large-scale IT systems in the Area of Freedom, Security and Justice, eu-LISA, sought our guidance regarding the significant risks associated with biometric matching technologies used in the Entry Exit System (EES) and the Shared Biometric Matching Service (sBMS), and on the measures to mitigate these risks.

We evaluated eu-LISA's need to adhere to legally required high accuracy standards, the potential risks to data subjects, and the inappropriateness of synthetic data for ensuring the matching engine's precision. Consequently, we allowed the extraordinary use of sampled VIS production data to guarantee the biometric matching engine's legal compliance concerning EES accuracy specifications.

In this context, before commencing operations, we mandated eu-LISA to enhance the DPIAs for both the sBMS and EES, as well as implement supplementary measures for the accuracy measurement process. These measures encompassed addressing risks arising from bias (e.g. age, gender, and ethnic origin), performance deterioration, and lack of synchronicity between various systems, in addition to establishing the minimal required amount of genuine biometric data for accuracy evaluations.

4.7.5.

Supervising data protection in criminal justice

We have worked closely with EPPO and Eurojust to ensure their compliance with data protection law, in particular in the application of data protection safeguards to protect individuals.

Supervision of EPPO

In 2022, the EDPS and EPPO continued to develop their relationship with an operational visit that took place in April. Presentations and on-the-spot demonstrations of how personal data is processed by EPPO were carried out, helping us gather knowledge about the agency's systems, practices and procedures. Meetings with European Prosecutors, European Delegated Prosecutors, EPPO staff and their DPO also provided us with additional material for further analysis and preparation of EPPO audits.

Throughout the year, 19 bilateral meetings were organised between EPPO's DPO office and the EDPS, during which we provided advice on the set up of new systems, changes to EPPO's internal rules governing procedures with an impact on data protection, as well as their cooperation with external partners which may involve transfers of personal data.

Eurojust

With 24 meetings held with the DPO of Eurojust, our working relations with Eurojust were particularly intense, following the Agency's new role as European hub for preservation, storage and analysis of evidence in cases concerning core international crimes, such as genocide, crimes against humanity and war crimes. During these meetings, we discussed a variety of data protection issues - from prior-consultations to the development of a new case management system for the Agency to cooperate with external partners and ongoing complaints.

4.7.6.

EDPS takes legal action as new Europol Regulation puts rule of law and EDPS independence under threat

On 16 September 2022, we requested that the Court of Justice of the European Union (CJEU) annuls two provisions of the newly amended Europol Regulation (registered as Case T-578/22, EDPS v Parliament and Council). The two provisions, which came into force on 28 June 2022, have an impact on personal data operations carried out in the past by Europol. In doing so, the provisions seriously undermine legal certainty for individuals' personal data and threaten our independence.

These new provisions, Articles 74a and 74b, have the effect of legalising retroactively Europol's practice of processing large volumes of individuals' personal data with no established link to criminal activity. This type of personal data processing is something that we had found to be in breach of the Europol Regulation, which we made clear in its Order issued on 3 January 2022 requesting Europol to delete concerned datasets within a predefined and clear time limit.

We noted that the co-legislators have decided to retroactively make this type of data processing legal, therefore overriding the EDPS Order. When data was collected under the previous Europol Regulation, individuals could expect that if their personal data was transmitted to Europol, Europol would be obliged to check within six months whether there was a link to criminal activity. Otherwise, as instructed by us, this data was supposed to be erased at the very latest by 4 January 2023. The new provisions of the Europol Regulation allow Europol to continue processing the data that has not yet been erased, despite our Order.

The co-legislators' choice to introduce such amendments undermines the independent exercise of powers by supervisory authorities. The contested provisions establish a worrying precedent with the risk of authorities anticipating possible counter-reactions of the legislator aimed at overriding their supervision activities, depending on political will. Data protection supervisory authorities, in this case the EDPS, could be compelled to consider political preferences or may be subject to undue political pressure in a manner that undermines their independence as enshrined in the EU Charter of Fundamental Rights.

CHAPTER FIVE

A safer digital future for the EU

By acting as an advisor to the EU legislators 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.

In 2022, we provided recommendations, through Opinions and Formal Comments, on a number of matters and topics: from the EU Media Act, Cybersecurity to Health and the EU's security.

Evolution of Legislative Consultations:

	2018	2019	2020	2021	2022
OPINIONS	8	7	10	12	27
JOINT OPINIONS	0	1	0	5	4
FORMAL COMMENTS	15	5	20	76	49
INFORMAL COMMENTS	33	16	14	29	30
TOTAL	**56**	**29**	**44**	**122**	**110**

5.1.
Protecting democracy and media freedom

A topic on which we provided advice and recommendations, mostly through a series of EDPS Opinions, were on measures designed to protect democracy and media freedom. Our advice aimed to enhance the protection of individuals' privacy, on a wide range issues, including the protection of individuals from profiling and behavioural targeting in the context of political advertising.

Profiling and targeting are practices that are particularly invasive and harmful to individuals as they are known to pose real challenges to their privacy and data protection rights. Combatting these issues is one of the core objectives laid down in our EDPS Strategy 2020-2024.

Online targeting for political advertising

We issued an Opinion on the Proposal for a Regulation on transparency and targeting for political advertising, in which we advocated for stricter rules in this area, in addition to proposed measures to make this type of advertising more transparent.

Our advice was particularly relevant given that political communication is essential for citizens, political parties and candidates in order for them to be able to fully participate in democratic life. The recommendations we provided aim to contribute to preserving our democracy, for which we believe strong rules to combat disinformation, voter manipulation and interferences with our elections, are necessary. To achieve this, we shared measures, and encouraged the EU Legislators, to do more to tackle the many risks surrounding the use of targeting and amplification techniques for political purposes.

To this end, we recommended that the proposed Regulation includes a full ban on micro targeting for political purposes, a practice consisting of targeting an individual, or a small group of individuals, with political messages according to some of their perceived preferences or interests that their online behaviour may reveal.

We also believe that the EU Legislators should consider further restrictions concerning the categories of personal data that may or may not be processed for the purpose of political advertising, including when political advertising involves the use of targeting and amplification techniques.

The EU Media Freedom Act

We also issued an Opinion on the EU Media Freedom Act.

Whilst supporting the objectives to protect media freedom, independence and pluralism across the EU, we called for better protection of journalists, and a ban on highly advanced military-grade spyware.

Our recommendations were therefore aimed at making the objectives of the EU Media Freedom act more effective in practice, to protect journalists, their sources, and media service providers.

In this respect, our recommendations were twofold. Firstly, to clarify that any journalist would benefit from the protection offered by the proposed Media Freedom Act. Secondly, to further define and restrict the possibility to waive the protection of journalistic sources and communications, particularly the exceptions related to the prohibition of intercepting communications using spyware or other forms of surveillance of media service providers.

Our Opinion also focused on the measures guaranteeing the independence of EU Member States' authorities and bodies tasked with reviewing breaches of the protection of journalistic sources and communications.

Pegasus: examining privacy risks

As a follow up to the revelations made in media reports about the use of Pegasus by several EU Member States, one of the most powerful hacking tool to date causing great concern, we issued Preliminary Remarks on modern spyware. The remarks we made aim to contribute to the EU's ongoing assessment of this technology, as well as inform EU citizens of the risks that this tool could pose.

Because this tool can be used to gain complete and unrestricted access to a person's device, such as a mobile phone's files, messages and other content, without their awareness, to spy on or even impersonate someone, we highlighted that the level of interference with the right to privacy is so severe that the targeted individual is in fact deprived of this right.

Our assessment also includes a proposed course of action, including a ban on the development and the deployment of spyware with the capability of Pegasus in the EU, strengthening democratic oversight over surveillance measures, strict application of the EU legal framework on data protection, or strengthening the protections offered by criminal procedure, to name a few examples.

5.2.
The Data Act

We issued a Joint Opinion on the EU Data Act, which aims to establish harmonised rules on the access to, and use of, data generated from a broad range of products and services, including connected objects ("Internet of Things"), medical or health devices and virtual assistants.

The field of health is an example in which new opportunities for data use is created. It is our responsibility to ensure that data is processed according to European values to shape a safer digital future, where individuals are protected, especially the most vulnerable.

With this in mind, together with the EDPB, we advised the EU legislators to provide limitations or restrictions on the use of data generated by the use of a product or service by any entity other than individuals, in particular where the data at issue is likely to allow precise conclusions to be drawn concerning individuals' private lives, or would otherwise entail high risks for the rights and freedoms of individuals.

We also jointly recommend introducing clear limitations regarding the use of the relevant data for purposes of direct marketing or advertising; employee monitoring; calculating, modifying insurance premiums; credit scoring, advising that these limitations are extended to protect vulnerable people.

We made other recommendations on the relationship between data protection and the enforcement of the proposed Regulation, such as on the oversight mechanisms.

5.3.
Health

Another topic in which our advice was sought is Health.

The proposal for the European Health Data Space

We also issued a Joint Opinion with the EDPB on the EU Health Data Space in which we advocated for strong protection of electronic health data.

The EU Health Data Space aims to facilitate the creation of a European Health Union and to enable the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data.

Together with the EDPB, we expressed several concerns, notably on the secondary use of electronic health data.

Health data generated by wellness applications and other digital health applications are not of the same quality as those generated by medical devices. Moreover, these applications generate an enormous amount of data, can be highly invasive, and may reveal particularly sensitive information, such as religious orientation. We therefore recommended that wellness applications and other digital health applications are excluded from being made available for secondary use, further highlighting the risks to the rights and freedoms of individuals that this may pose.

Alongside this, we stressed the need to add as a requirement that electronic health data be stored in the EEA. This is contingent on the fact that the infrastructure for the exchange of electronic health, foreseen in the Proposal, will process enormous amounts of highly sensitive data and as such will require utmost surveillance and protection from unlawful access.

We provided other recommendations on the supervision of the functioning of the EU Health Data Space.

Extending the EU Digital COVID Certificate

Pursuing our monitoring of data protection during COVID-19, we issued a Joint Opinion with the EDPB on the extension of the EU Digital COVID Certificate in the context of travels within the EU.

The EU Legislators' Proposals in this area are of particular importance due to their major impact on the protection of individuals' rights and freedoms. Any restriction to the free movement of individuals within the EU to limit the spread of COVID-19, including the requirement to present EU Digital COVID Certificates, should be lifted as soon as the epidemiological situation allows.

We therefore highlighted in our Joint Opinion of the need to continuously evaluate which measures remain effective, necessary and proportionate, in the fight against the COVID-19 pandemic. Further underscoring that data protection principles should be continuously applied and integrated, having due regard to the evolution of the epidemiological situation and the impact on fundamental rights.

5.4.
Exchanging personal data to combat crime

The access to relevant information by law enforcement authorities and the exchange of information between law enforcement authorities is key to effectively combatting crime.

To this end, we issued several Opinions on legislative proposals related to the criminal justice area.

Additionally, in cases of international cooperation, we remained vigilant in ensuring that international agreements are compatible with EU data protection law and standards.

5.4.1.
EU Police Cooperation Code

We published two Opinions on the Commission's Proposal for the Regulation on automated data exchange for police cooperation ("Prüm II") and on the Proposal for a Directive on information exchange between law enforcement authorities of Member States. Both Proposals are part of the "EU Police Cooperation Code" package. We shared recommendations to the EU Legislators on the two proposed Regulations.

We made a series of recommendations, given the risks associated with the processing of individuals' personal data in criminal matters, on the necessity and proportionality of the envisaged measures should be clearly demonstrated, so that the level of protection for individuals guaranteed by EU law is not undermined.

Regarding the Proposal on the "Prüm II Regulation", we stressed that the proposed new framework lacks essential elements related to its material and personal scope, such as the types of crimes, which may justify a query, and the categories of individuals affected by the automatic exchange of data.

Regarding the Proposal for the Directive on information exchange, we stressed the need to clearly define the personal scope of the measure, and in any event, to limit the categories of personal data about witnesses and victims that may be exchanged. In addition, we highlighted the risk of creating a vast database of back-copies of exchanged information at Europol, as an unintended result of the envisaged default involving of the Agency in the exchanges between Member States.

5.4.2.
Exchanging personal data to fight crime and terrorism

We issued an Opinion on a proposed Agreement between the EU and New Zealand on the exchange of personal data between Europol and the authorities of New Zealand competent for fighting crime and terrorism.

This Opinion is a continuation of our prior work commenced in 2020 when we released Opinion 1/2020 on the negotiating mandate for the present Agreement, where we took into account, amongst other factors, the specific situation of New Zealand and its well-developed national data protection system.

Overall, we concluded in our 2022 Opinion that the Agreement between the EU and New Zealand, which enables the transfer of sensitive personal data of potential criminals between Europol and the competent authorities of New Zealand for fighting serious crime and terrorism, provides adequate safeguards with respect to the fundamental right to privacy of individuals.

Data protection and war crimes

In May 2022, we issued an Opinion regarding the collection, preservation and analysis of evidence relating to genocide, crimes against humanity and war crimes at Eurojust, done outside of Eurojust's existing case management system (CMS).

We measured the importance of delivering this Opinion in a timely way, given that Eurojust's activities aim to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to core international crimes, including those committed following Russia's military aggression against Ukraine on 24 February 2022.

For Eurojust to be able to carry out its work in this area, there is an urgent need to address the limitations of the current Eurojust CMS, because, in general, personal data related to crimes must only be processed within this CMS. Given that the current CMS does not have the technical capacity to centralise evidence on core international crimes in an efficient and secure manner and the new CMS is still to be established, we considered that this derogation of the use of CMS should be of a temporary nature and that the automated data management and storage facility should be integrated into the new CMS, once established. In addition, we provided several recommendations with a view of ensuring the level of data protection as already guaranteed by the Eurojust Regulation is not undermined.

Combatting child sexual abuse online

In our Joint Opinion with the EDPB on preventing and combating child sexual abuse (CSAM), we emphasised the serious and heinous crime that is child sexual abuse.

We highlighted that limitations to the rights to private life and data protection must, however, respect the essence of these fundamental rights and remain limited to what is strictly necessary and proportionate.

Whilst supporting the goals and intentions behind the Proposal, we consider that it may present more risks to individuals, and, by extension, to society at large, than to the criminals pursued for CSAM.

The lack of detail, clarity and precision of the conditions for issuing a detection order for CSAM and child solicitation does not ensure that only a targeted approach to CSAM detection will effectively take place. There is a risk that the Proposal could become the basis for a generalised and indiscriminate scanning of content of virtually all types of electronic communications. We therefore advocated for the conditions for issuing a detection order should be further clarified.

International Cooperation to fight crime

We issued an Opinion on two Proposals: one to authorise EU Member States to sign the Second Additional Protocol to the Budapest Convention on Cybercrime, and the other to authorise EU Member States to ratify this same Protocol.

Whilst investigating and prosecuting crime is a legitimate aim, for which international cooperation, including the exchange of information, plays an important role, we emphasised the importance for the EU to have sustainable agreements for sharing personal data with non-EU countries for law enforcement purposes. These agreements should be fully compatible with EU law, including the fundamental rights to privacy and data protection.

To this end, our recommendations focused on the management and monitoring of non-EU countries' access to personal data linked to crime. For example, amongst our recommendations, we advised that requests, from non-EU/EEA countries, that are party to the Protocol, for accessing specific types of information, which could pose a significant risk to the fundamental rights to privacy and data protection, should only be granted if they are transmitted to the authorities of the Member States and not directly sent to service providers.

In the same vein, we issued an Opinion on a future UN Convention on cybercrime.

We expressed concerns about the UN Convention, because, in its current form, it could potentially weaken the protection of individuals' fundamental rights, given the large number of countries, which each have their own legal system, that are partaking in its negotiations. As such, we advised the EU not to become party to the future UN convention on cybercrime, if its final draft does not guarantee these fundamental rights.

Our additional recommendations included the following:

- the exchange of personal data between countries should be limited to the crimes defined in the future UN Convention;
- access to and exchange of personal data should be monitored carefully and should only occur between law enforcement authorities of the concerned countries;
- agreements between EU and non-EU countries guaranteeing greater protection of individuals' privacy rights than the UN Convention should take precedence; and
- an EU Member State should, in certain cases, be allowed not to cooperate under the international convention with a non-EU country party to the future UN Convention.

5.5. Cybersecurity

Cybersecurity goes hand-in-hand with data protection. They are two essential allies for the protection of individuals' data. In 2022, we issued several Opinions pertaining to this topic, with the aim to contribute to uniforming cybersecurity regulations and policies within and beyond the EU.

These Opinions are also part of our wider work in the field of technology monitoring, to help ensure that cybersecurity products with digital elements embed the principles of data protection by design and by default, to protect the fundamental rights of individuals.

Towards EU-wide cybersecurity requirements and rules

We issued three Opinions on proposed Regulations that aim to bring about EU-wide cybersecurity requirements and rules, as part of the EU's Cybersecurity Strategy.

In particular, we issued an Opinion on a proposed Regulation laying down cybersecurity requirements for products with digital elements, such as browsers, operating systems.

In the Opinion concerning the first Proposal, we emphasised the importance of having measures that would ensure an appropriate level of security when personal data is processed. In relation to this point, we strongly recommended that data protection by design and by default principles are part of the requirements set out in the proposed Regulation.

As part of having EU-wide cybersecurity requirements, the Proposal provides for a European cybersecurity certificate. In response to this measure, we made it clear that this certification does not mean that products with digital elements are compliant with the General Data Protection Regulation, and does not replace the GDPR certificate either.

In our second and third Opinions on measures for a high common level of cybersecurity and information security in the EU institutions, bodies, offices and agencies (EUIs), we stressed the importance of integrating the privacy and data protection perspective in the management of cybersecurity and information security. We also highlighted the risks for compliance with the EU privacy and data protection legislation that are implied by the security measures mandated by the Proposal.

5.6.
Artificial Intelligence

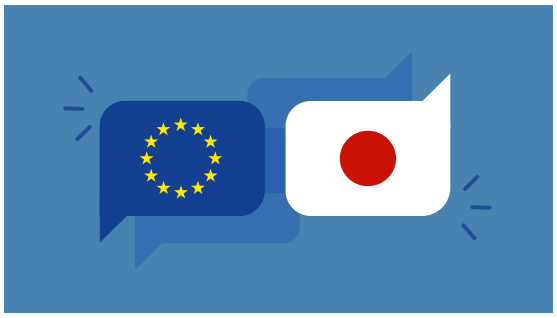
As highlighted in our EDPS 2020-2024 Strategy, Artificial Intelligence (AI) is increasingly deployed in public services and criminal justice. Our role is to ensure that this new technology is used in compliance with EU data protection law and respects individuals' privacy.

In addition to other initiatives we have produced, or participated in, we issued an Opinion on the Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention an international Convention on artificial intelligence, human rights, democracy and the rule of law (AI Convention).

We consider this AI Convention as an important opportunity to develop the first legally binding international instrument on AI according to the European standards and values on human rights, democracy and the rule of law, complementing the EU Artificial Intelligence Act.

To achieve this aim, the AI Convention needs to include appropriate, strong and clear data protection safeguards to protect individuals who may be affected by the use of AI systems.

5.7.
International Partnerships



As part of our work in supporting partnerships between EU Member States and other non-EU countries, to promote and facilitate the EU's economic growth for example, we issued an Opinion on EU's Agreement for an Economic Partnership with Japan.

Like many other partnerships of this nature, the EU-Japan economic agreement may involve the exchange and processing of individuals' personal data, such as tax data and information linked to the identity of company holders. We were therefore consulted on the data protection implications of transfers of information.

In our Opinions we shared that since the European Commission had granted an Adequacy Decision, recognising that Japan provides an adequate level of data protection, and exempting further authorisations for transfers of personal data, we recommended to further explain why further negotiated provisions for personal data transfers were necessary.

5.8.
Justice and Home Affairs

Justice and Home Affairs is a policy field in which we routinely provide advice and recommendations, as it deals with issues that require recurrent important aspects related to the EU's security and its citizens, such as combatting crime, terrorism, freedom of movement, often involving the processing of individuals' personal data, including sensitive information, which we aim to protect.

5.8.1.
Interoperability in practice

We provided advice on the interoperability of certain EU large-scale IT systems.

The European Travel Information and Authorisation System

One of the large-scale database systems that is part of the interoperability framework is the European Travel Information and Authorisation System (ETIAS) Regulation. ETIAS is put in place to support the delivery of travel authorisations for visitors of visa-exempt countries to enter the Schengen Zone, which includes most EU countries. In this regard, we were consulted by the European Commission on the technical specifications that should be put in place to ensure compliance with the data retention requirements set out in ETIAS.

In our Opinion, we provided advice on how to carry out checks to ensure compliance with data retention rules.

Another example of our work in the context of large-scale IT systems' interoperability and its impact on data protection are our Formal Comments on the European Commission's Delegated Decision which specifies the conditions for the correspondence between the data in an application file stored in the ETIAS Central System, and the data present in a record, alert or file of the following EU information systems: ETIAS, Visa Information System (VIS), Schengen Information System, Entry Exit System, European Criminal Record System. In these Formal Comments, we recommended, for example, to process only the personal data that is strictly necessary to be able to determine whether identities are similar or the same.

5.8.2.
Security, Safety and data protection

In addition, we provided more specific advice on the use of certain of the EU's large-scale IT systems.

Risks related to security, illegal immigration, or high epidemic risk

We were consulted by the European Commission on defining the risks related to security, illegal immigration, a high epidemic risk, for a draft Delegated Decision.

The draft Decision mainly focused on algorithmic profiling as well as the determination of the criteria for assessing the risk for short stay and long stay visa, as well as residence permit applications.

We recommended that the European Commission further defines what constitutes a security, illegal migration and high epidemic risk in line with the requirement set in the VIS Regulation - the system that allows exchange of visa data - rather than limiting the draft Decision to setting out the modalities by which such risks could be defined.

Furthermore, in a view to ensure a proportionate application of risk profiles and to avoid arbitrary and discriminatory targeting of groups of travellers, we strongly suggested that the definition of a precise methodology, clear criteria and strong safeguards, are included in the process of compiling risks and risk profiles.

Schengen Area: disclosing criminal convictions

We were also consulted on the type of questions that applicants should reply to in their application form when applying for a travel authorisation to the Schengen area (ETIAS). Questions included, for example, information on previous criminal convictions over the last 15 years, or over the last 20 years if a conviction is related to a terrorist offence.

Amongst our recommendations, we advised to:

- reduce the time periods related to a possible previous criminal convictions so as to align them with the time periods provided for in the basic act;
- remove the envisaged obligation of the applicant to provide personal data of family members or friends as part of the application form, which is considered to be excessive and not justified;
- reconsider the methodology for the establishment of the list of specific war and conflict zones to make the selection more targeted and objectively linked to possible security or other risks for the EU.

This works aims to ensure that data protection requirements are integrated into all new legislation composing the interoperability framework and to ensure appropriate oversight and review.

The digitalisation of visa procedures

We issued an Opinion on a proposed Regulation on the digitalisation of the visa procedure which seeks to simplify and harmonise visa application procedures within the Schengen area.

Supporting the aims of the Regulation, we signalled that it may create additional obstacles to visa applicants, for instance, due to IT illiteracy or lack of adequate equipment. Highlighting this issue, we recommended including in the Proposal an explicit provision that would exempt individuals with accessibility issues from using the European digital visa application platform.

We provided other recommendations on the importance of only processing personal data needed for a specific purpose, and to ensure fair and transparent processing by providing information to individuals on how their personal data is used.

CHAPTER SIX

Technology Monitoring & Foresight

We place strategic importance in integrating the technological dimension of data protection into our work. Technology developments can make society advance, and increase the well-being of individuals, but, at the same time, this progress has the potential to increase and exacerbate privacy and data protection risks. Therefore, we believe it is our role, as the data protection authority of EU institutions, bodies, offices and agencies (EUIs), to not only raise their awareness, but also the public's, to the risks that current, emerging, and new technologies may pose to people's privacy.

Our efforts in 2022, already pursued in previous years, were three-fold. To contribute to developing core knowledge by anticipating and understanding the possibilities, challenges, and impact of emerging and new technologies through Foresight. Develop effective oversight mechanisms to monitor the development of technologies in a privacy-friendly way. Cooperate with other data protection and technology experts, as well as other EUIs, to promote the integration of privacy throughout the development of technologies, to protect individuals' fundamental rights. These objectives are aligned with our EDPS Strategy 2020-2024.

6.1. 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 change in light of data protection.

In this regard, our efforts in 2022 were fuelled by the need to ensure that from the earliest stages of conception, technologies are designed with data protection and privacy features at the forefront. In doing so, we focused our energy in helping Europe become more resilient and future-proof, as per our objectives set out in the first pillar of our EDPS Strategy 2020-2024 on Foresight.

With Foresight, we aim to offer practical guidance and insight on the impact of the design, evolution, potential risks and deployment of digital technology on the fundamental rights of individuals.

6.1.1.
TechSonar: anticipating emerging technology trends

One of the ways we practice Foresight is through TechSonar, an initiative that we launched in September 2021 to anticipate emerging technology trends, their value and risks for society, instead of reacting to these trends, once they are developed.

TechSonar is a process that allows us to continuously analyse the technology arena with the aim of selecting tech trends it foresees for the near future. Simply put, our ambition is to prepare, as much as possible, for technological evolutions by mapping out some of the plausible scenarios that emerging technologies may create, particularly their implications on data protection and individuals' privacy.

From a methodological standpoint, we select the technologies worth monitoring by going through the following phases:

- initial scouting of trends;
- collective brainstorming;
- collective review;
- publishing and advocacy; and
- continuous monitoring.

In our first TechSonar Report 2021-2022, we explored six foreseen technology trends, namely smart vaccination certificates, synthetic data, central bank digital currency, just walk-out technology, biometric continuous authentication and digital therapeutics.

Our second TechSonar Report 2022-2023 re-examined synthetic data and the central bank digital currency. In this second TechSonar edition, we also evaluated fake news detection systems, the Metaverse, and federated learning. For both of these reports, we provide a summary of each technology, its impact on our day-to-day lives, as well as its possible effects on individuals' privacy.

By creating TechSonar, we aim to influence the development of new and emerging technologies in a privacy-friendly way. This initiative also serves as a compass for future and more in-depth activities, both by the EDPS itself and other data protection authorities (DPAs) within the EU and beyond.

6.1.2.
Anticipating technologies together

In addition to initiatives like TechSonar, we engage with experts in the legal and technology domains through events and other activities, in order to proactively align technological advancements with EU data protection standards. Exchanging views with other professionals helps us inform our work, and combine different approaches to fostering privacy-compliant technologies that respect individuals' data.

Panelfit conference

On the 30 and 31 March 2022, together with the Vrije Universiteit Brussel, the EDPS held the closing event of Panelfit - Participatory Approaches to a new Ethical and Legal Framework for ICT, which is a H2020 EU-funded project that focuses on "Anticipatory Compliance". The concept of anticipatory compliance involves proactive anticipation of practical ways of regulating new or emerging technologies, so that they align with EU data protection law. Contributing to the event, we highlighted that next to ensuring legal compliance, acting in advance fosters innovation and supports the value-creation that these technologies offer.

Anticipatory enforcement

With the support of the Brussels Privacy Hub, we organised a workshop on anticipatory enforcement in June 2022 to create awareness on foresight and anticipatory techniques applied to data protection enforcement practices. The workshop was organised on the margins of the EDPS Conference 2022, "The Future of Data Protection: Effective Enforcement in the Digital World" (See Chapter 8).

Our motivation for organising this workshop was four-fold. To define anticipatory enforcement; identify the building blocks of anticipatory enforcement; design speculative scenarios of implementation of anticipatory enforcement in Europe; outline the steps to operationalise anticipatory enforcement in the context of the EDPS and the overall data protection landscape.

Participants of the workshop - from academia, private and public sectors, regulators, authorities, and civil society - engaged in discussions about hypothetical scenarios where enforcement is carried out proactively, without waiting for risks to arise, or a situation of non-compliance to manifest itself. In total, we developed four plausible scenarios set in 2030 that aimed to provoke uncertainty and uncomfortable feelings amongst participants to provoke discussions and reactions. During the discussion, participants stressed that these scenarios were fully plausible, frightening and stimulating a sense of urgency.

The main outcome of the workshop was that effects of privacy violations might not be visible in the short-term, therefore, individuals may not be aware of the effects that might rather materialise in the long term. In this sense, foresight and anticipatory techniques can become important tools that contribute to raising awareness amongst individuals about the long-term effects of these privacy violations. What is more, it emerged that a continuous and structured dialogue amongst the different data protection stakeholders, especially enforcement agencies and bodies, is necessary. This would allow for greater clarity in the application of data protection rules. Participants agreed that the use of foresight methodology could support this dialogue.

6.2.
Monitoring technologies to improve data protection compliance

By monitoring technologies' development and their impact on the privacy and protection of individuals' personal data, through various initiatives pursued over the years and continued in 2022, like TechDispatch, we are able to provide informed and comprehensive advice to EUIs using ICT tools and other technologies to carry out their day-to-day tasks, whilst protecting people.

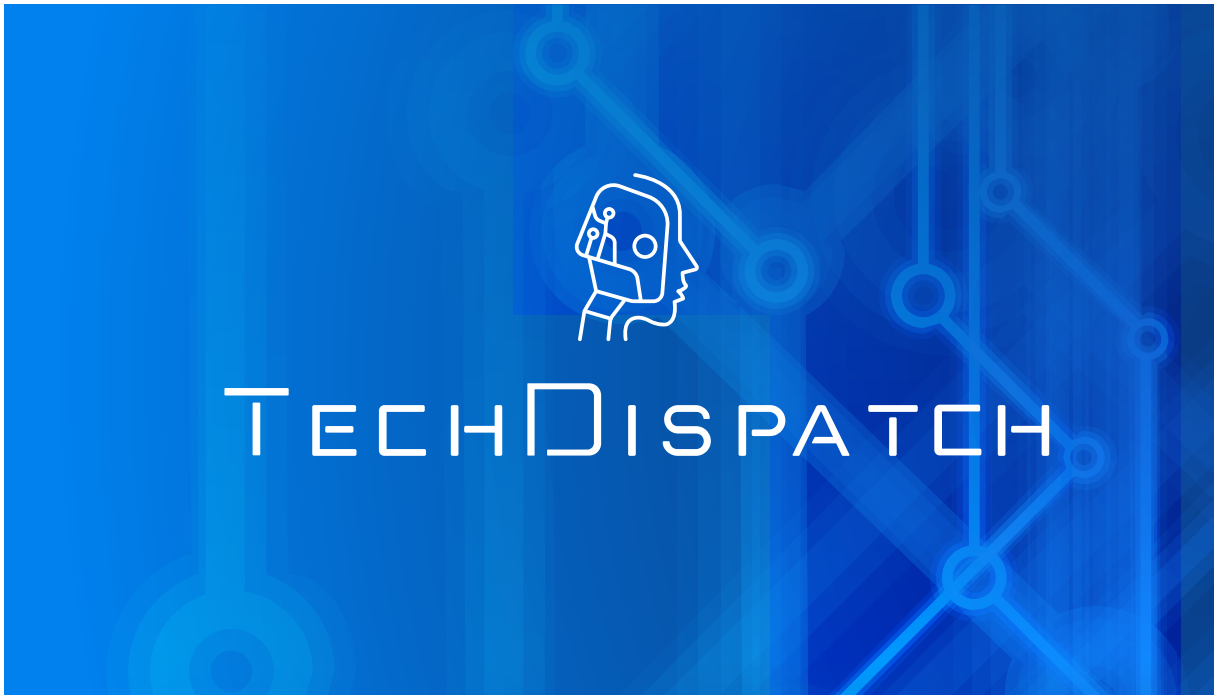
6.2.1.
TechDispatch Reports

In 2019, we created TechDispatch.

TechDispatch is a publication series which has received high recognition, by winning a Global Privacy Award in the category for Education and Public Awareness in 2021. It is composed of reports created to explain, inform and raise awareness of potential data protection issues surrounding new technologies. Each TechDispatch provides factual descriptions of a new technology, assesses its possible impact on privacy and personal data protection, and provides links to further recommended reading.

With these reports, we aim to foster ongoing dialogue on new technologies and data protection challenges, whilst at the same time promoting the incorporation of data protection by design and by default within innovation processes.

This initiative is part of the EDPS's wider activities on technology monitoring. Our TechDispatch edition of 2022, issued by our Technology and Privacy Unit, focused on the topic of Fediverse and Federated Social Media Platforms.



Federated Social Media Platforms

The Fediverse consists of many social media platforms that are both independent from each other as well as being interoperable with one and another, therefore allowing users to interact with each other across different platforms. Because of the nature of these social media platforms, they are also known as federated social media platforms. In our TechDispatch, we breakdown some of the advantages, opportunities and challenges that federated social media platforms present in the context of data protection, and how these compare to traditional centralised, non-interoperable social media platforms.

6.3.
Promoting cooperation and knowledge-sharing

Conducting our work efficiently in measuring the impact of technologies on data protection cannot be achieved without cooperating, learning from and sharing knowledge with other data and technology experts, regulators, authorities, and other EUIs. Putting this into practice, we fostered productive discussions, participated in a wide variety of events, and other initiatives, throughout the year, on a multitude of topics, including artificial intelligence, digital identity, cybersecurity, EU digital currency and more.

6.3.1.
Podcasts: an interactive way to discuss technologies

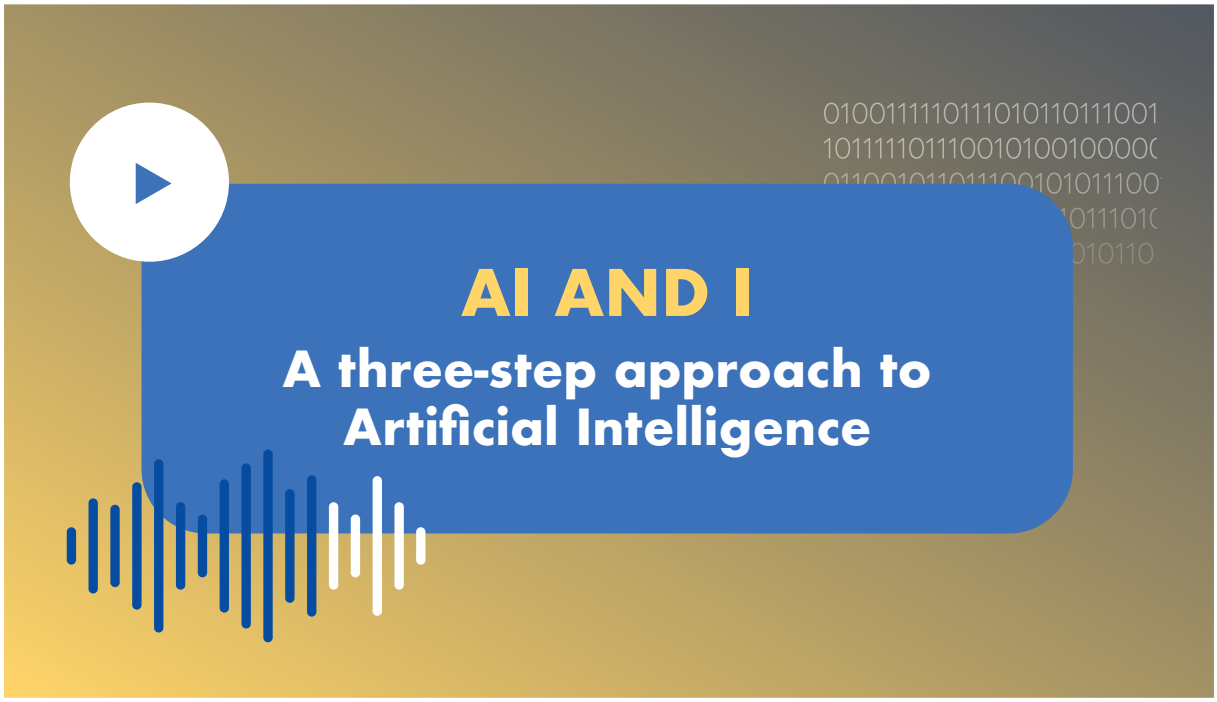
In recent years, to broaden the reach of our work and engage with a larger audience, we have been producing various podcast series. This has enabled us to inform the public about our activities as well as engage in insightful discussions with experts from various fields. A popular format that we have often pursued is a three-part podcast series on various topics of interest, directed by EDPS and EDPB trainees, with our support. In 2022, two three-part podcast series were produced, one delving into the EU's digital ID wallet and the other examining artificial intelligence (AI).

Delving deeper into the EU Digital Identity Wallet

The impact of the EU Digital Identity (ID) Wallet on individuals' data protection and privacy rights has been a central focus of our work since 2021. This technology aims to facilitate the online identification of EU citizens with administrative agencies, as well as help them efficiently to carry out transactions of private nature by safeguarding electronic versions of their personal documents. If implemented in line with the principle of data protection by design and by default, the technology might provide EU citizens with control over who has access to their digital ID and what personal data is disclosed.

AI and I: a three-step approach to Artificial Intelligence

AI has gradually become an important part of our daily lives and entails the processing of huge volumes of personal data. Undeniably, this presents risks that must be addressed through appropriate laws, technological safeguards and EU-wide collaboration. Due to AI's complex nature, we considered it important to create a podcast series to expand the public's knowledge on the topic. Similarly to the one on the EU Digital ID Wallet, the episodes provide a granular approach to AI. In the first episode of the three-part podcast series, EDPS and EDPB trainees provide an introduction to the topic of AI, including reflections on how the use of AI may evolve in the future. In episode 2, the inherent risks posed by AI to human rights, for example, discrimination effects, is examined. The last episode focuses on the various approaches to help regulate AI, ensuring that individual's fundamental rights are respected.



6.3.2.
Dispelling myths on Machine Learning

In September 2022, we published "10 Misunderstandings on Machine Learning", an initiative we worked on with the Data Protection Authority of Spain - Agencia Española de Protección de Datos (AEPD), as part of a long-standing collaboration in which we aim to dispel misunderstandings on technologies and their impact on data protection.

Machine Learning is a branch of artificial intelligence used to help resolve specific and limited problems, such as classifying and predicting tasks. To achieve these results, machine learning models are trained using relatively large volumes of data. Once trained, these systems use the patterns learned to produce their output. Therefore, the performance of machine learning models depends greatly on the accuracy and representativeness of the data used. On a day-to-day basis, machine learning models may be applied to social media, virtual personal assistance, self-driving cars, for example.

In just a few short pages, the EDPS and the AEPD aim to help you bust some of the myths linked to machine learning, such as:

- Are machine learning systems less subject to human biases?
- Can machine learning systems improve over time?
- How accurate and qualitative should the data used to train machine learning systems be?

Other publications part of this series include, "14 misunderstandings on biometric identification and authentication" and "10 misunderstanding on anonymisation".

6.3.3.
Pairing up cybersecurity and data protection efforts

In 2022, the EDPS and ENISA - the EU Agency for Cybersecurity formalised its collaboration, which has been ongoing for several years, in a signed Memorandum of Understanding (MoU), a strategic document to address together issues of common concern, such as cybersecurity, as a way of protecting individuals' personal data.

Based on the MoU, we jointly agreed to consider 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).

The plan also aims to promote a joint approach to cybersecurity aspects of data protection, to the assessment and possible adoption of privacy-enhancing technologies, and to strengthen the capacities and skills of EUIs.

ENISA Annual Privacy Forum: analysing the privacy of technologies

Each year, new privacy and data protection risks and opportunities of technological developments and relevant EU policy initiatives are assessed at the Annual Privacy Forum (APF).

As a key partner of the two-day forum organised by ENISA, we contribute to these conversations with other panellists - from technology to policy experts - by taking a solution-focused approach. Our input covers data protection engineering and privacy enhancing technologies.

Other topical discussions in which we participated this year involve technological research, advancements in AI, the role of legal research in the work of a supervisory authority, and how cookies and a privacy-by-design approach can coexist during website design.

By partaking in these important discussions, we are given the opportunity to engage with other members of the data protection community, exchange views, learn new approaches as well as share best practices related to data protection, which in turn help inform our work.

Cyber Europe: preparing for crisis management

In 2022, we participated in ENISA Cyber Europe, a bi-annual series of exercises simulating large-scale cybersecurity incidents, such as personal data breaches, in certain business areas to test the level of preparation of the EU in cyber crisis management.

Our involvement this year was particularly pertinent, since the exercises focused on the simulation of incidents involving personal data in the medical sector, which may involve special categories of data, such as health data, which is particularly sensitive and requires special measures when processed to protect individuals. During the exercises, we engaged in discussions on the actions participants responded with to evaluate the overall preparedness of the medical sector. Contributing to this initiative helps us shape our efforts and understand how players, like EUIs, handle personal data breaches caused by cybersecurity incidents. It is imperative that EUIs put in place procedures that protect individuals' personal data, and that they also put in place effective mitigation measures and contingency plans.

In the coming years, we will continue raising awareness on personal data breaches management and strengthening collaboration with ENISA to ensure that data protection aspect are incorporated in cybersecurity exercises, like this one.

6.3.4.
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 IPEN, we organise webinars and in-person events bringing together technology and data protection experts, such as academics, regulators, open source and business developers, to launch and support projects that build privacy into everyday tools and to develop new tools that can effectively protect and enhance our privacy.

In addition, IPEN was also created with the idea to increase awareness of the technologies that help protect personal data.

To this end, we organised two IPEN events, one on Digital Identity and another one on Central Bank Digital Currency, throughout 2022.

Complementing our policy work on the EU Digital Identity Wallet, we organised an IPEN event during which views were exchanged regarding the compatibility of digital identity solutions with data protection; its relevant challenges and opportunities.

During the event, we stressed the importance of developing systems and solutions that cultivate trust and accountability to prevent mass surveillance and safeguard individuals' fundamental rights to privacy and data protection in the digital world.

Our second IPEN event of the year 2022 focused on Central Bank Digital Currency. Organising this workshop was particularly apt given that 90 per cent of central banks around the world have already explored a state-owned digital currency with different design choices; the European Central Bank has also started exploring this option and is planning for an assessment by 2024.

Amongst the topics discussed, the IPEN webinar focused on the process of validating transactions. Namely, who would be involved in this process, what would be their role, and can this process ensure that the privacy of individuals making payments is protected.

Other topics explored during the event included the technology requirements necessary to develop a digital currency that is privacy compliant and effective; how to monitor and audit these technologies; how to prevent the creation of "fake digital money".

6.4.
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 European institutions, offices, bodies and agencies (EUI) have a duty to report personal data breaches to us, 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, EUIs must also inform the concerned individuals without unnecessary delay. These obligations also apply to breaches concerning operational personal data. Whilst Chapter 9 of Regulation (EU) 2018/1725 introduces the data breach notification requirements for operational data, additional requirements for notifying competent national authorities may be introduced in the EUIs' own Regulations, as is the case for Europol - the EU Agency for Law Enforcement Cooperation and Eurojust - the EU Agency for Criminal Justice Cooperation, for example. For the European Public Prosecutor's Office, similar notification requirements are introduced by Regulation (EU) 2017/1939.

Risk assessment is a core element in preventing and responding to personal data breaches. Unlike other traditional security risk assessment methodologies, the focus in a personal data breach is evaluating the risk to the rights and freedoms of individuals. Whilst various stakeholders, supervisory authorities and private and public organisations use a range of different methodologies to assess this risk, our data breach Guidelines, currently being updated, aim to simplify the task by providing guidance and practical examples to assist EUIs in this area.

In this context, in 2022, we organised two (2) workshops with the EUIs' network of Data Protection Officers. The workshops focused on the upcoming update of the EDPS Guidelines and on how EUIs should notify us when a personal data breach has occurred, which gave rise to fruitful discussions and helpful feedback from data protection officers. We also organised 2 online talks, in cooperation with the European School of Administration (euSA), to raise the awareness of EUIs' employees on assessing and notifying personal data breaches. During these talks, we also covered the most frequent scenarios in which a personal data breach may occur, such as addressing a letter or an email to the wrong recipient, or more complex yet, errors when handling transparency and access to document procedures. A similar, tailored training was organised in the European Parliament, for the Directorate-General for Communication. Training sessions provide EUIs' employees and data protection officers with ideas on how to minimise or avert risks in some of these situations.

6.4.1.
Notifications in Numbers

In 2022, we received and assessed 95 new personal data breach notifications under Regulation (EU) 2018/1725. Overall, there was a 9% increase compared to 2021, during which we received 87 personal data breaches.

Table 1: EDPS - Number of Personal Data Breach Notifications for the years 2019-2022

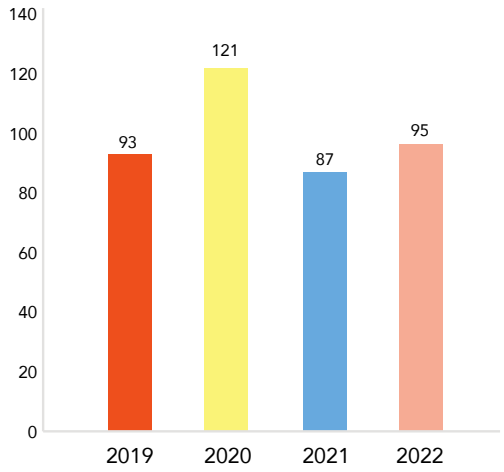
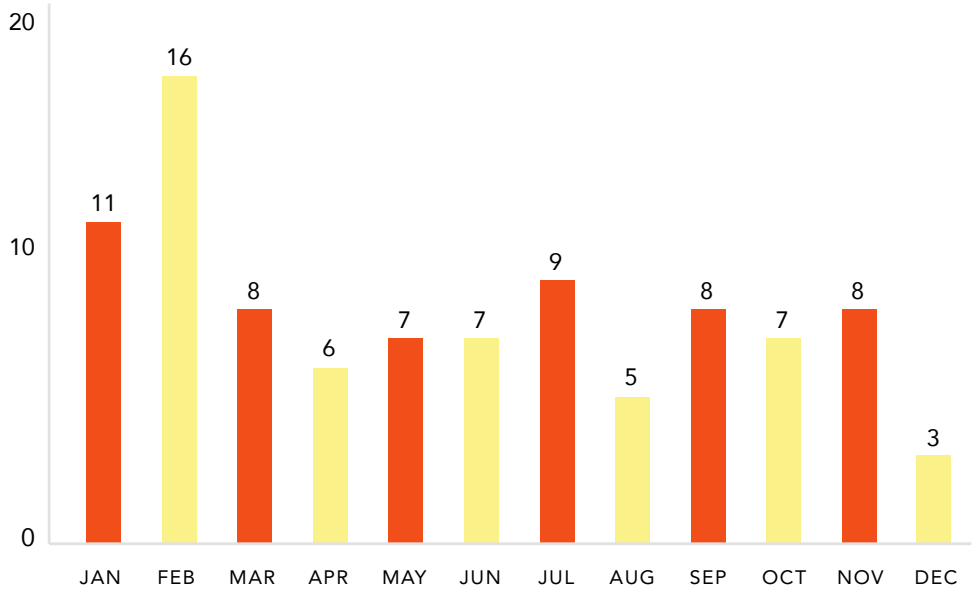


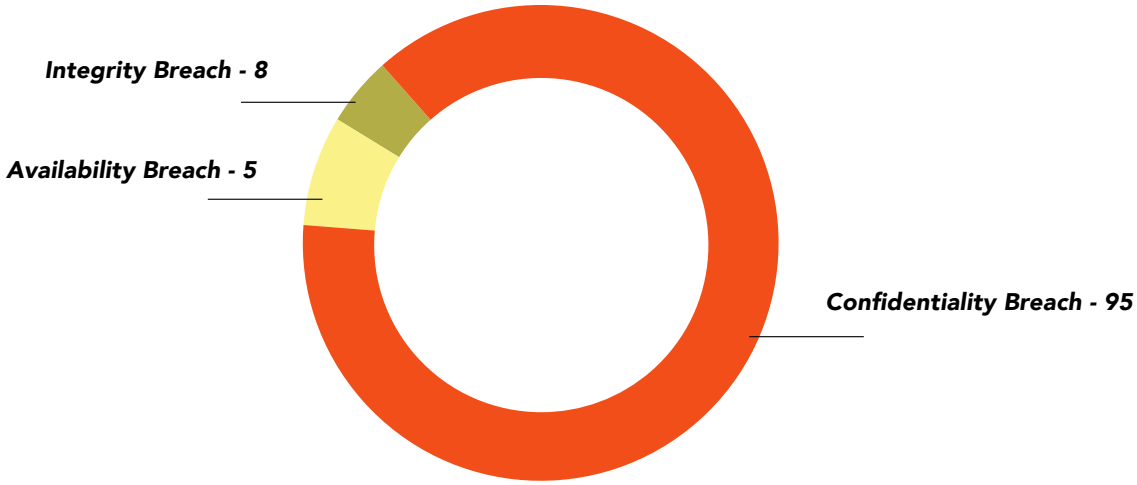
Table 2: EDPS - Number of Personal Data Breach Notifications per month for the years 2019-2022



6.4.2.
Type of Personal Data Breaches in 2022

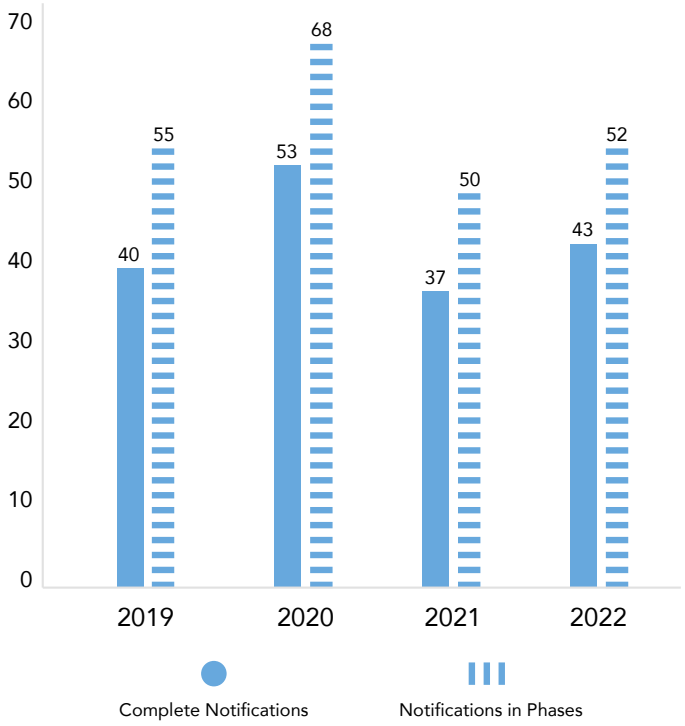
A personal data breach may result from either a confidentiality, availability or integrity breach or a combination of the above. All the notified personal data breaches in 2022 concerned a breach of confidentiality. 8 cases included an integrity breach and 5 cases included availability breaches.

Table 3: EDPS - Type of Personal Data Breaches 2022



In 2022, we received 52 comprehensive data breach notifications and 43 notifications in phases. At the end of 2022, not all notifications in phases had been finalised from the relevant EUIs. As shown below, the proportion of comprehensive notifications and notifications in phases did not differ significantly in comparison to previous years.

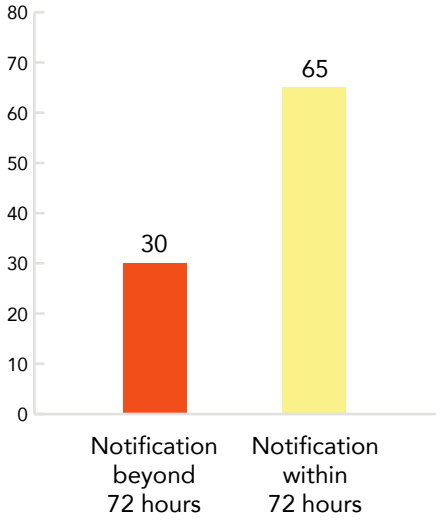
Table 4: EDPS - Type of Data Breach Notification - Category complete/in phases - Years 2019-2022



6.4.3.
Notification within 72 hours

65 notifications were submitted within 72 hours, whilst 30 notifications were delayed due to various reasons. In some cases the delay was justified, for example in cases where investigations were still ongoing to identify how individuals' personal data was affected. In some other cases, delays occurred due to lengthy internal procedures of approval of the notification. In the latter case, we advise the EUIs to review and simplify their internal processes for data breach notification, so that unnecessary delays can be avoided.

Table 5: EDPS -Type of Data Breach Notification - Category complete/in phases - Years 2019-2022



6.4.4.

Root Cause of Personal Data Breaches in 2022

Examining this year's root causes of personal data breaches, human error remains the most common cause, with an increase of 9% from the previous year. Cases included, sending an email to the wrong recipients or putting all recipients in copy whereas their contact details were not to be disclosed to the rest of the recipients list. In the same vein, we also received data breach notifications concerning the publishing of documents without removing personal data, in the context of EUIs' access and transparency procedures. Similar to previous years, a high number of human errors during recruitment processes were notified. Nevertheless, the errors were not always related to the fact that EUIs continued to hold recruitment processes online. In some cases, results of the selection process were sent to erroneous candidates.

At the same time, a high number of data breaches due to a human error, involving the sending of medical invoices to wrong recipients, were also notified to us.

External attacks were the second 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 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 data retention periods had been put in place.

The fact that external attacks exploiting personal information stored in the information systems of the EUIs have increased in 2022, means that EUIs need to review and strengthen their security measures and related processes.

Furthermore, data breaches caused by technical errors decreased by 7% compared to 2021. The most usual type of technical errors enabled access to documents one should not have access to.

Table 6 : EDPS - Root Cause of the Personal Data Breaches 2022

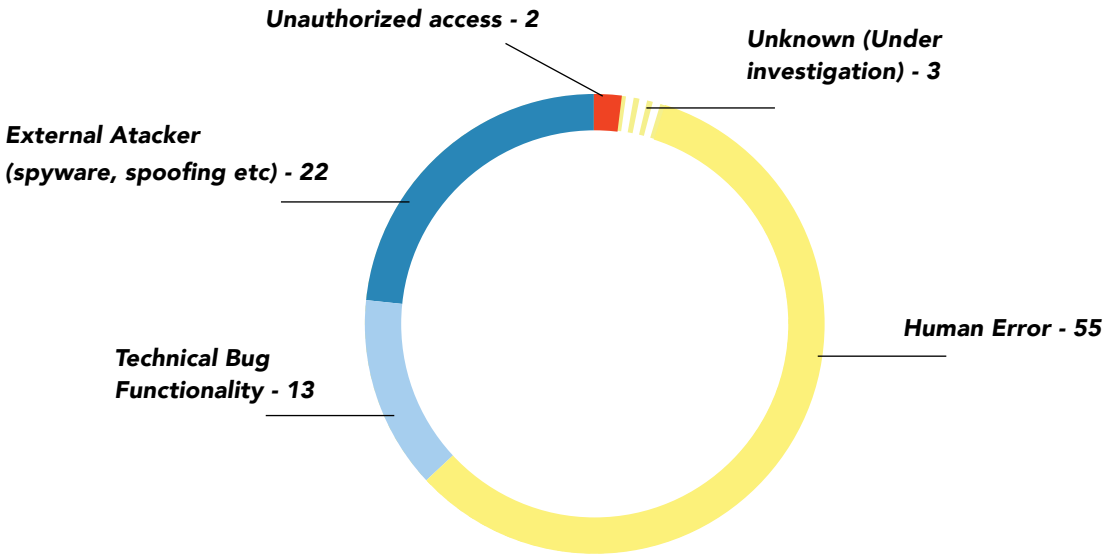
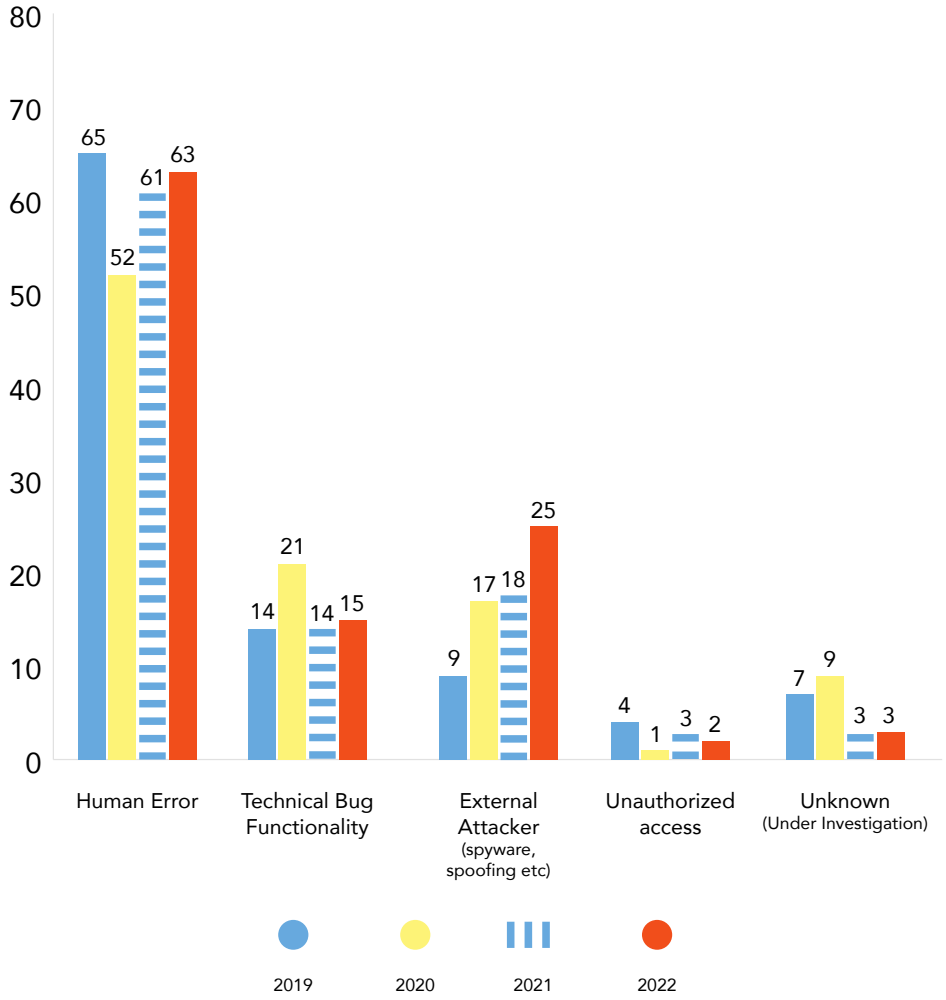


Table 7 EDPS -Comparison Chart on the Root Cause of the Personal Data Breaches 2019-2022

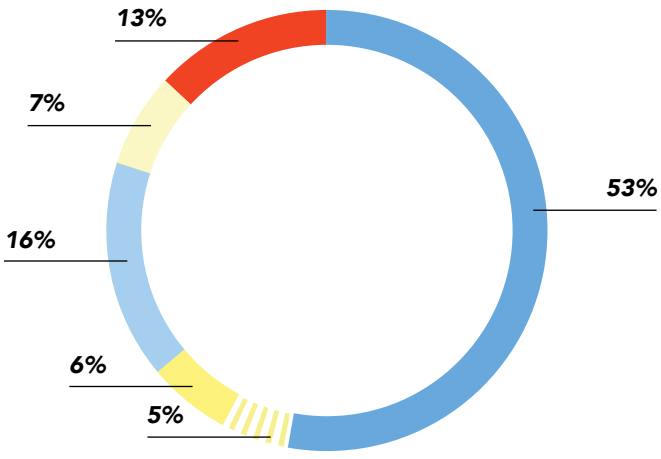


6.4.5.

Number of affected individuals of Personal Data Breaches in 2022

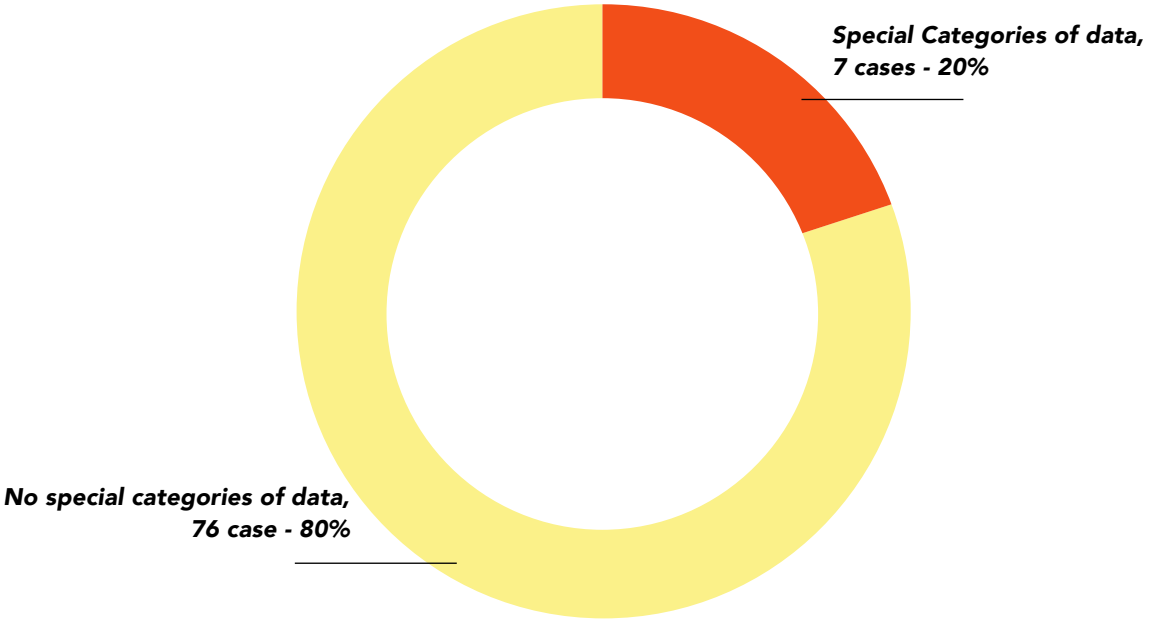
In the majority of cases - 53% approximately -a small number of individuals - between 1-10 - were affected, whilst in 16% of cases, 101-500 data subjects were affected. In 12 cases of personal data breaches, more than 1000 individuals were affected, which equals to 13% of the total cases.

Table 8: EDPS - Number of affected individuals of Personal Data Breaches in 2022



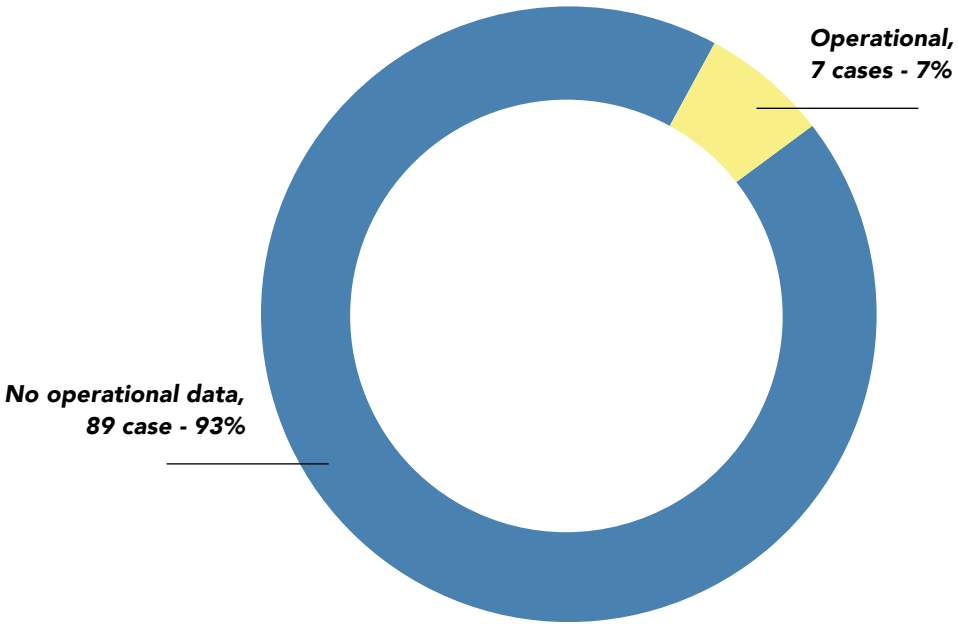
6.4.6.
Categories of Data in Personal Data Breaches in 2022

Table 9: EDPS - Special Categories of data - Personal Data Breaches 2022



20% of the data breach notifications received this year involved special categories of data. In the majority of cases, breaches involved health data, like errors when sending medical invoices, during the reimbursement processes. We recommend EUIs to raise their staff's (or contractors) awareness, and to consider additional safeguards to avoid human error.

Table 10: EDPS - Operational data - Personal Data Breaches 2022



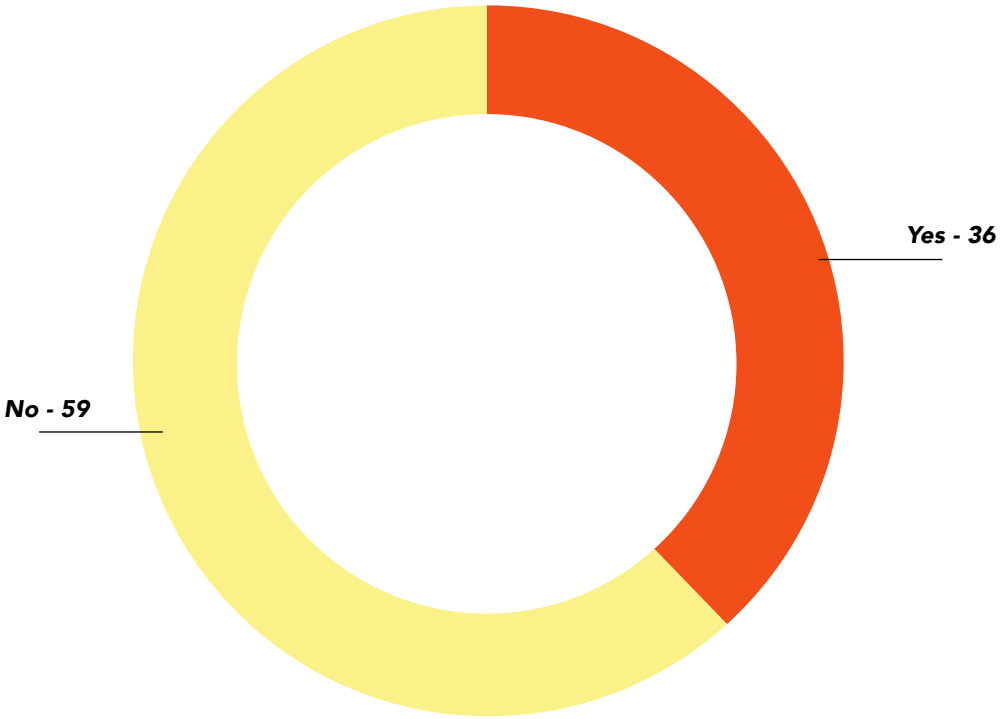
In 7% of the personal data breach cases, confidentiality of operational data was affected. The categories included suspects and individuals under investigations, as well as information related to officers being assigned specific tasks. Concerning the operational data breach notifications we received, no special categories of data were concerned. Concerning this category of breaches, we took a precautionary stance and included a data breach case affecting the confidentiality of information received on allegations of crime, as it was not clear from the initial analysis of the controller which of these allegations had resulted in the opening an investigation.

6.4.7.
Communicating data breaches to individuals

In 36 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 2022, there were four (4) cases in which we assessed that the incident was of high risk, which was in contradiction to the EUI's initial assessment, and we therefore asked them to notify individuals' concerned. In all 4 cases, the notification to individuals were made.

Table 11: EDPS -Notification to the Data Subject - Personal Data Breaches 2022



6.4.8.
Other data breach notifications

We also received notifications outside our competence.

We received fourteen (14) not notifiable personal data breach cases from EUIs. In these cases, we assessed there was unlikely risk posed to individuals and therefore informed EUIs to document the breach in their internal register. We also received nine (9) notifications sent from private companies or individuals (whistle-blowers), which were outside the scope of Regulation (EU) 1725/2018. These were either from companies having a main establishment in the EU, in which case the national Supervisory Authority under GDPR would be competent, or from companies processing data of EU citizens, without an establishment in the EU.

CHAPTER SEVEN

Achieving Together

One of our core aims of this year, and this EDPS Mandate, is to ensure the consistent and coherent application of EU data protection law and standards across the EU Member States and the European Economic Area (EEA), and beyond.

To achieve this, we carry out, lead and participate in various initiatives.

We cooperate closely with the EU/European Economic Area's (EEA) data protection authorities in the European Data Protection Board (EDPB), which promotes consistent data protection across the EU.

We also engage with international stakeholders to foster solution-focused discussions, share best practices on data protection matters, through international fora, events.

7.1.
Working with the EDPB

The EDPB is composed of the EU's and EEA's data protection authorities, including the EDPS.

We are not only a member of the EDPB, but we also provide its Secretariat, which includes logistical support, financial resources, as well as legal expertise on data protection matters, a Memorandum of Understanding guides our cooperation.

Through this platform, we have initiated and participated in various activities together with the other EU/EEA Member States, such as the Coordinated Enforcement Action, Coordinated Supervision Committees and groups, on matters related to border management for example.

7.1.1.
Coordinated Enforcement Action

February 2022 marked the launch of the EDPB's Coordinated Enforcement Action, in which we participated, together with 22 other data protection authorities of the EU/EEA, by focusing on the compliance of EU/EEA entities, and EU institutions, bodies, offices and agencies (EUIs), with EU data protection law when using cloud-based services, especially when these are sourced from entities outside the EU/EEA. We first proposed this topic after identifying the need for closer cooperation and action to ensure data protection compliance in this area, in particular regarding the controller-processor relationship and international transfers when public sector bodies use cloud-based services.

Building on common preparatory work done by all participating data protection authorities, our focus is to ensure EUIs' compliance on this issue through a series of actions, such as fact-finding exercises, questionnaires to identify if a formal investigation is warranted, launch of investigations, following-up on ongoing investigations on the use of cloud-based services. Following these actions, we were able to garner an understanding of the issues encountered by EUIs, as well as examples of best practices, which we could share with the other data protection authorities.

We contributed to this initiative as part of our goal to ensure that organisations within the public sector at national and EU level lead by example when it comes to outsourcing services and transferring personal data within and outside the EEA, by continuously putting in place effective measures to protect individuals' personal data according to EU standards.

The findings of the participating authorities and their recommendations for public bodies on the use of cloud services are available in the EDPB Report on the 2022 Coordinated Enforcement Action, published in early 2023.

Upcoming Coordinated Enforcement Action

In addition to this Coordinated Enforcement Action, preparations are underway for the launch of a second coordinated enforcement action on the designation and positions of data protection officers in 2023, to which we are actively participating in, by sharing our knowledge experience, best practices, based on our collaboration with EUIs' data protection officers, through our well-established EDPS-DPO network for example.

7.1.2.
Strengthening cooperation with EU data protection authorities in the Area of Freedom, Security and Justice

Joint supervision by the EDPS and the EU Member States' data protection authorities is key, in particular in the Area of Freedom, Security and Justice, since EUIs process personal data collected at national level, which is then further shared by competent national authorities of the EU Member States, for the performance of their tasks. This currently takes place under the umbrella of the Coordinated Supervision Committee (Europol, Eurojust, EPPO) and the Supervision Coordination Groups.

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 Schengen Information System and the Visa Information Schengen - all 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 recasts of the Eurodac and VIS Regulations.

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

Coordinated Supervision Committee

To this end, we actively participated in Coordinated Supervision Committee, which organises the joint supervision of Europol - the EU Agency for Law Enforcement Cooperation, Eurojust - the EU Agency for Criminal Justice Cooperation and EPPO - the European Public Prosecutor's Office.

Our efforts focused on continuing to jointly ensure that data processed by Europol about minors under the age of 15, who are classed as suspects or potential criminals, is in line with the law of the EU Member State that is sharing this personal data, as well as with the requirements set out in the Europol Regulation.

This joint supervisory activity, ongoing since 2020, is something we initiated on the basis of our 2018 Europol Annual Inspection. Complementing this initiative, we carried out similar checks regarding the processing of data of minors classed as potential criminals or suspects submitted by non-EU/EEA countries and international organisations, as part of our 2022 Annual Inspection of Europol. We check that Europol is only processing the data of minors who have reached criminal responsibility by sharing and comparing statistics with the responsible authorities of the EU/EEA. This has been effective since we have noticed a drop in numbers over the years.

Participating in Supervision Coordination and Groups

We also participated in other Supervision Coordination Groups, and Boards, together with the data protection authorities of the EU Member States.

The Visa Information System Supervision Coordination Group

As part of our participation in the Visa Information System (VIS) Supervision Coordination Group (VIS SCG) together with the data protection authorities of Germany, Czech Republic, Hungary, the Netherlands and Poland, we contributed to the preparation of a common inspection plan for the Visa Information System.

This activity, which is part of the Working Program 2019-2021 of the VIS SCG, aims to provide assist data protection authorities in their supervisory role. Concretely, our contribution aimed to bring a common approach to VIS inspections, when analysing findings for example. This plan serves as a guide to data protection authorities, whilst taking into account EU Member States' own laws, specificities, procedures or methodologies.

By participating in this endeavour, we contribute to ensuring a consistent and coherent application of EU data protection law.

The European Police Record Index System pilot project

In connexion with our two Legislative Opinions that we issued in March 2022 on the Police Cooperation Code Package, which aims to facilitate the exchange of information for law enforcement and police cooperation, we came to learn about an ongoing EU-funded pilot project to establish a European Police Record Index System (EPRIS), through a prior consultation submitted by Europol. The pilot project includes a consortium of several EU Members States, as well as Europol, and aims to develop a system for automated searching and exchange of police records.

As the prior consultation lacked a coordinated Data Protection Impact Assessment by the participating authorities and the assurance that with national supervisory authorities had been consulted, we shared our Supervisory Opinion with the BTLE subgroup, used to coordinated action with the national supervisory authorities concerned when legislative work is ongoing. The work conducted intends to make sure that the system developed adequately addresses data protection risks. This work contributed to the EDPB statement on the European Police Cooperation Code.

7.1.3.
Providing technical support to the EDPB

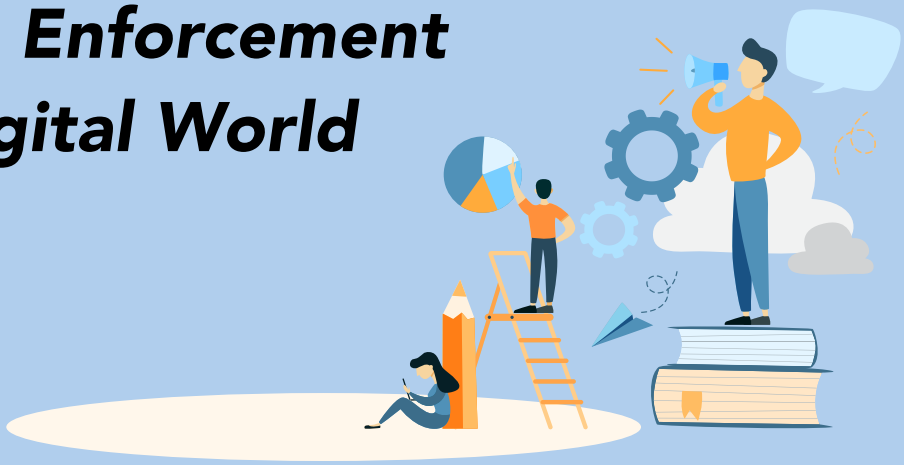
We provided technical support to the EDPB in the auditing of open-license websites, by equipping them with appropriate tools, such as our Website Evidence Collector, which we initially launched in 2019 and have constantly been improving and updating since then, adding a number of features, and fixing technical bugs and glitches for example. Using this tool, as a basis, has allowed the EDPB to build a new website audit tool for their own activities.

In the same vein, we shared with the EDPB technical documents to help them set up the mobile app audit lab: an infrastructure to carry out mobile app audits, for them to not only use, but also share with the Board members - the EU Member States' data protection authorities, to ensure consistent practices across the EU. As an added layer of support, we volunteered to animate an EDPB expert group, that meets a few times every year, in which representatives of data protection authorities of the EU 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 started the organisation of a workshop to provide more in-depth training to data protection authorities' staff, to arm them with the necessary skills and tools in this area - with the aim of pursuing this initiative in 2023.

CHAPTER EIGHT

EDPS Conference 2022: The Future of Data Protection: Effective Enforcement in the Digital World



The impetus for the EDPS to host a conference was born out of the EDPS 2020-2024 Strategy. In the Strategy, the wheels were set in motion for us to host a conference discussing how to safeguard effectively individuals' rights to privacy and data protection, as enshrined in the European Union Charter of Fundamental Rights.

In planning and putting together this conference, we wanted to create a platform to bring the world's best practices together, and steer meaningful discussions about the future of the digital regulatory sphere. At the heart of this desire was the acknowledgment that there should always be scope for discussion on how to potentially improve the enforcement of data protection rules, as they are crucial to the safeguarding of fundamental rights.

On 16 & 17 June 2022, this conference became a reality. Titled "The Future of Data Protection: Effective Enforcement in the Digital World", the conference brought together over 2,000 participants, both in Brussels and online. Featuring over one-hundred speakers; three main sessions; sixteen breakout sessions; nine individual keynote remarks; and five side events, the two-day event fostered crucial conversations on the future of data protection, with a particular focus on the enforcement of the General Data Protection Regulation (GDPR).

As explained by Wojciech Wiewiórowski in his keynote speech: *"We wanted to come back to the drawing board, to sit down together with all of you and reach conclusions that can inform the public debate. The public deserves this. Things that can be defined now should be defined now, not in an unspecified future"*.

The richness of the debates at the Conference exceeded our expectations. The conversations kick-started during the panels of the conference kindled broader reflections on current approaches that continued to unfold for the months following the Conference.

We are proud that the conference has been an important factor in the developments related to the functioning of the GDPR - starting with Vienna Summit Statement of the EDPB, then the so-called "EDPB procedural wish-list", and the European Commission's announcement on the planned legislation harmonizing certain procedural aspects of cross-border cooperation.

We see them as achievements of the whole data protection community, "*committed, passionate and able to continuously find ways to improve*" - as expressed by Wojciech Wiewiórowski during his closing remarks at the Conference. Whilst the two-day event was a way to reflect on the past and present, ultimately we believe our Conference served as an important roadblock for the future of data protection: "*I deeply believe that a closer integration is needed if we are serious about protecting EU citizens' personal data across the EU. We are weaker when divided, and stronger together*", said Wojciech Wiewiórowski.

We encourage you to read our Conference Report, where you can find a summary of the conversations, reflections, keynote speeches, workshops and side events held during these memorable sunny days in Brussels.

CHAPTER NINE

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 on data protection matters.

Council of Europe

The Consultative Committee of the Convention 108 (T-PD) is responsible for the interpretation of the provisions of the Convention 108, the first legal binding international instrument in the data protection field, and to facilitate and improve its implementation. 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; digital contact tracing; 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.

With the modernisation of the Convention 108, a very important and strategic follow-up mechanism to the Convention will be created, also creating additional tasks for the T-PD. We also 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. 38 ratifications are indeed necessary for the entry into force of this unique and landmark instrument.

Still at the Council of Europe, we partake 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.

Spring Conference

The data protection authorities of EU Member States and the Council of Europe meet annually for a 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 to promote cooperation between the different systems in Europe, and between the professionals who work within these systems and to exchange best practices.

A delegation of the EDPS participated in the 30th edition of the European Conference of Data Protection Authorities (Spring Conference), held from 18-20 May in Croatia.

The EDPS was actively involved in the preparation of this event. We organised and spoke on a panel on "Foresight, innovation and technology monitoring", and moderated another panel on "Enforcement cooperation: cross-border cases and Article 50 of the GDPR, mutual assistance between EU and non-EU countries".

Members of the Spring Conference also adopted a resolution to accelerate the ratification of the Convention 108+ and adopted a second Resolution on the Conference Vision, Mission and Steering Group for the Spring Conference. An interim Steering Group was set up and EDPS has been appointed as member of this Group.

The Spring Conference also welcomed two new members, the DPA of Lower Saxony and the European Space Agency and a new observer: the EDPB.

Global Privacy Assembly

We took part in the 44th Global Privacy Assembly, hosted by the Personal Data Protection Authority of Turkey (KVKK) in Istanbul (Turkey), between 25 and 28 October 2022.

The Global Privacy Assembly (GPA), previously named International Conference of Data Protection and Privacy Commissioners, is an international forum with more than 130 data protection and privacy authorities from across the globe that gather to connect and share their perspectives on the developments in data protection and key elements of their international cooperation.

During the 44th edition of the GPA, a number of resolutions were adopted:

- Resolution to Amend the Road Map and the Timeline;
- Resolution on International Cooperation Capacity Building for Improving Cybersecurity Regulation and Understanding Cyber Incident Harms;
- Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology.

To find out more about the 44th Global Privacy Assembly, its reports and resolutions, please consult this webpage on the EDPS website.

Organisation for Economic Cooperation and Development

The work of the OECD is becoming increasingly relevant for the EU and the EDPS.

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 in particular 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 linked 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) and follows the activities of the Working Party on Artificial Intelligence Governance (AIGO).

Of particular importance are two Declarations adopted at the OECD ministerial meeting held on 14-15 December 2022 on a Declaration on a Trusted, Sustainable and Inclusive Digital Future and a Declaration on Government Access to Personal Data Held by Private Sector Entities, the first intergovernmental agreement in this area.

Roundtable of G7 data protection and privacy authorities

We participated in a Roundtable of G7 Data Protection Authorities organised in Bonn, Germany, between 6 and 8 September 2022.

This event was organised by the Federal Data Protection Authority of Germany in the context of the German Presidency of the "Group of Seven", an inter-governmental political forum consisting of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, as well as the European Union. The EU was represented by the EDPS, Wojciech Wiewiorowski, and the Chair of the European Data Protection Board (EDPB), Andrea Jelinek.

At the event, the G7 data protection authorities discussed a wide range of topics, including:

- the "data free flow with trust" concept;
- the intersection of privacy, competition and consumer protection;
- international data transfer tools;
- privacy-enhancing technologies and de-identified data;
- the use of principles of data minimisation and purpose limitation to meet the challenges of commercial surveillance;
- the role of privacy and data protection authorities in the setting and promoting of an ethical and cultural model for the governance of artificial intelligence.

International Organisations workshop

On 12-13 May, we co-organised with the World Food Programme the 2022 edition of the International Organisations workshop, in Rome, Italy.

Initiated in 2005, our objective for these workshops is to provide a platform to bring together international organisations to share experience, practice and analysis of common challenges.

This rationale appears to be more relevant than ever in 2022, with over 100 participants and more than 50 organisations represented at the workshop.

In the first panel session, various stakeholders participated and exchanged perspectives about legal, policy or technological updates related to privacy and data protection. The second panel session was devoted to individuals' data protection rights, specifically enforcement, governance, challenges and opportunities for international organisations. The workshop concluded with a session on the tension between innovation and data protection, considering the challenges including anonymisation, role determination, security, data sharing, for instance in AI, cloud computing or Blockchain.

The discussions on both days of the workshop demonstrated the commitment of the international organisations' data protection community. We will continue to support their efforts and continue to contribute to increasing global cooperation.

To find out more about the International Organisations workshop, visit our relevant webpage.

The Berlin Group

Each year, the International Working Group on Data Protection in Technology (IWGDPT), also known as the Berlin Group, meets to discuss, in particular, data protection and privacy issues related to information and technology.

The Berlin Group, established in Germany in 1983, is composed of representatives of DPAs around the world, including the EDPS, as well as independent experts representing various sectors, such as public authorities, private organisations, academia and civil society.

This year the Group met twice, in June in Tel Aviv (Israel) and then in November in London (UK). Both meetings were opportunities to exchange main experiences and expertise as to technology monitoring and advance on guidance papers on subjects commonly chosen.

In London, the EDPS and the UK ICO presented their foresight methodologies and deliverables, both much appreciated. The Group decided that the future work and its guidance papers on technological impact be somehow driven by the outcome of those activities, considered as a strategic contribution.

As part of the Group's activities, we also provided substantial feedback on the upcoming facial recognition paper and on the telemetry paper, and will lead the drafting of the paper on Central Bank Digital Currency.

CHAPTER TEN

Communicating 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.

10.1.
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, more recently, by organising regular social media campaigns, for example. Likewise, we continue to communicate on the EDPS' priorities on our main platform, the EDPS Website.

10.1.1.
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 Twitter, LinkedIn and YouTube, which we use to reach a global audience easily and quickly.

Our @EU_EDPS Twitter account allows us to promote the EDPS' presence at a variety of events and to feature the core messages and purpose of our work. Our latest tweets are always available to view on the homepage of the EDPS website.

We use our **European Data Protection Supervisor LinkedIn account** to communicate with data protection specialists and other actors interested in the field of data protection. With this communication channel, we reached a new milestone this year, by surpassing over 63,000 followers at the end of 2022. 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. This medium was an essential tool in promoting our EDPS Conference on The Future of Data Protection: Effective Enforcement in the Digital World, before, during, and after the event to retrace and highlight the important discussions held at the time.

10.1.2.
Launching new social media channels: EU Voice & EU Video

With the aim of seeking alternative communication tools that promote a more democratic, decentralised and privacy-friendly model of social media, we launched a public pilot phase for two social media platforms: **EU Voice** and **EU Video**, as additional communication channels to our **Twitter** and **LinkedIn** accounts.

On **EU Voice**, we publish short posts about ourwork, 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.

These two platforms, based on free and open source Mastodon and Peertube software, are built on open standards. By launching this pilot phase, we aim to contribute to the European Union's strategy for data and digital sovereignty to foster the independence of the public sector in the digital world, as well as complying with EDPS recommendations on privacy by design.

By using these platforms, and encouraging their use, we aim to help shift the ownership of social media platforms from a handful of private entities to users will be beneficial to citizens and to the democratic processes of a data-driven society. Differently from the main traditional social media channels, these two platforms do not employ hidden algorithms that feed users with user-tailored, personalised content, therefore minimising conscious and unconscious biases. Users have reinforced freedom of choice on information.

10.1.3.
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 well-informed about our activities. Some of our social media campaigns were targeted towards promoting particular initiatives, such as our upcoming events, others allowed 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.

- **#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, twice a year, to raise awareness of less high-profile topics and to remind our audience about activities that they might have missed over the past year.

- **#EUvsDisinfo**: In March 2022, in the context of the Russian invasion on Ukraine, we partnered with EU vs Disinfo, a project led by European External Action Service, to better forecast, address and respond to the Russian disinformation campaigns affecting the EU. The campaign aimed to raise awareness about disinformation and the threats it poses to democracy.

- **#EDPSconf2022**: In June 2022, the EDPS hosted a high-level conference on the future of data protection. Preceding the event, we held a social media campaign promoting different aspects of the conference, to give an idea to potential participants a teaser of what they could expect during the conference, thus enticing them to register for this event. All panels, workshops and speeches were promoted on social media during the two days of the conference.

- **#TechSonar**: In September and October 2022, we held a campaign promoting one of the flagship projects of the Technology and Privacy Unit, TechSonar. Through this campaign we enhanced the project's visibility and purpose of presenting future tech trends.

- **European Cybersecurity Month**: In October 2022, we celebrated European Cybersecurity Month. To mark the occasion we prepared an extensive social media campaign raising awareness about cyber threats like phishing and ransomware.

- **Supervision Conference**: In November and December 2022, our social media efforts focused on producing an informative campaign explaining how the EDPS ensures the protection of personal data in the criminal justice area. This campaign supported the supervision conference we co-organised with Eurojust and EPPO.

10.1.4.
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.

Achieving this priority means we have carried out some more technical actions. For example, we completed the migration of our website to Drupal 9, which was started at the end of 2021. 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.

10.2.
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, 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 Director and the Supervisor share their reflexions on data protection.

10.2.1.
Monthly updates: 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 over 5000 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 2022, we published 7 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.

10.2.2.
Launching 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. In a way, 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.

10.2.3.
A more personal outlook on data protection

Now active for over six years, the EDPS blog is a platform through which the Supervisor, Wojciech Wiewiórowski, the Director and, more recently, 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 2022, we published 9 blogposts on an array of subject matters.

This medium has proved to be useful, not just in 2022, 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; and
- an insight into the EDPS-EDPB traineeship.

Blogposts that we published in 2022 also focused on the reporting the events organised by the EDPS. This included IPEN webinars, the EDPS-EDPB trainees' conference.

10.2.4.
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.

In 2022, we published two factsheets to raise awareness on cybersecurity matters, providing information in particular on ransomware and phishing, and the best practices to adopt to protect oneself from such threats. Other examples include a factsheet on some of our ongoing investigations, and one on individuals' key data protection rights.

10.3.
Public Relations

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

10.3.1.
Press Releases

This year we issued 28 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:

- EDPS Conference 2022 and the call for pan-European approach to GDPR enforcement,
- supervision activities of Europol and Frontex;
- online targeting for political advertising;
- COVID-19;
- cybersecurity, cybercrime and information security;
- media freedom and alternative social media;

- developments related to Artificial Intelligence, electronic health data, and other data acts;

- and several joint opinions with the EDPB.

All of our press releases are published on the EDPS and on the EU Newsroom websites. They are also distributed to our network of journalists and other interested parties.

10.3.2.
Media interest

The topics that garnered the most attention in 2022 are detailed below. They prompted all sorts of media inquiries, such as requests for follow-up interviews with the EDPS Supervisor.

- **Supervision of Europol**: Our enforcement actions concerning Europol's processing of large datasets attracted the most media attention. This was also the case with our legal action requesting that the Court of Justice of the European Union annuls two provisions of the newly amended Europol Regulation.

- **The EDPS' Conference in June 2022**: The conference on The Future of Data Protection: Effective Enforcement in the Digital World was one of the biggest privacy and data protection conference in the post-pandemic world, inevitably attracting media interest. Discussions revolved around the world's best practices when it comes to enforcement action and cooperation, while also exploring alternative models of enforcement for the future.

- **Joint Opinions with the EDPB**: The joint actions touched on a variety of topics, such as the EU Digital COVID Certificate, the EU Data Act, the European Health Data Space, and the rules to prevent and combat child sexual abuse.

- **Artificial intelligence and novel technologies**: Our publications, such as TechDispatch and TechSonar, address the impacts of new technologies on fundamental rights of data protection and privacy. Media coverage followed our publications requesting comments on related topics, such as federated social media, the metaverse, synthetic data or digital currency.

10.3.3.
Public requests

In 2022, 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, French or German; 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.

10.4.
Events

Picking up the pace after COVID-19, we are gradually increasing the number of events and study visits we organised.

EDPS Conferences

A highlight of our work was organising the EDPS Conference on The Future of Data Protection: Effective Enforcement in the Digital World, for which extensive communication and logistic support was provided. The Conference, a hybrid event, brought together more than 2000 participants (See Chapter 8).

Our work, which started in 2021, consisted of, for example, building a strong visual identity for the event, developing communication campaigns such as visuals, leaflets and videos, to explain and promote the conference, and engaging with journalists and stakeholders to promote the conference.

To enhance the Conference's visibility, we also created a dedicated website in English, French and German. This website not only served as a repository for us to manage registrations and other logistics, but also to facilitate participants' access to the Conference, its programme, photographs and latest updates. Similarly, we deployed a data protection friendly web-stream, to ensure that the conference was accessible to all.

To provide an opportunity to participate in the conference virtually, we wanted to ensure that all conference panels were livestreamed and recorded. The EDPS sought to design and put in place a videoconferencing and livestreaming service that provided not only a high-quality service, but also a service that fully respects data protection law, particularly regarding data transfers to countries outside the European Union (EU) and the European Economic Area (EEA).

With the aim of ensuring the smooth-sailing of this event, careful preparations went into choosing venues, the location, the design of signage and brand material, and the management of side-events organised on the margins of the Conference.

Building on this success, we organised at the end of November a conference on data protection in the field of criminal justice in the EU in cooperation with European Union Agency for Criminal Justice Cooperation - Eurojust, and the European Public Prosecutor's Office - EPPO. The event was attended by 300 participants, both remotely and in-person.

Leading up to the Supervision Conference, we organised a social media campaign, and other various communication activities dedicated to raising awareness on data protection in the area of criminal justice. The Conference itself demanded the detailed selection and organisation of venues, beverages, luncheons, presentations and on-hand availability to welcome participants.

Europe Day

Every year on 9th May, we celebrate Europe Day, marking the anniversary of the Schuman Declaration that brought peace and unity in Europe.

Being fully engaged in this celebration year upon year, we joined, together with the European Data Protection Board, we joined EUIs as they open their doors to the public to explain, in an interactive way, what they do and why. We prepared a stand full of playful activities - suitable to all ages - at Berlaymont Building of the European Commission.

EDPS Study Visits

Likewise, we organised study visits, which are an essential part of our communication strategy and connection to the public. With this initiative, started in 2010, we aim to raise awareness about our work and the importance of protecting the fundamental rights of privacy and data protection to small groups, often university students from across the EU, and beyond. This format allows us to meet and discuss about everyday data protection matters and transmit first - hand our knowledge, perspective, culture and values. Meeting small groups also allows to have more in-depth conversation tailored to students' interests and studies. In 2022, we organised 7 study visits with a total of 132 participants.

NOYB's presentation at the EDPS

On October 13th, we hosted Mr Max Schrems, Honorary Chairman of Non of Your Business (NOYB), who presented a software tool created by the data protection association, NOYB, which can automatically generate complaints concerning unlawful cookie banners. The presentation was directed towards the staff of the European Data Protection Supervisor (EDPS) and colleagues from several German Data Protection Authorities (DPAs) for the Catholic church. The presentation aimed to offer a detailed understanding of the software's functionality and legal analysis conducted by NOYB.

10.5.
Celebrating Data Protection Day

Each year, we mark data protection day with a week-long communication campaign.

Data Protection Day, held every 28 January, marks the anniversary of the Council of Europe's data protection convention, known as "Convention 108", the first binding international law concerning individuals' rights to the protection of their personal data.

The campaign we organised this year gained a lot of popularity and was very well received by the audience, which was particularly visible in a high number of reactions and engagement on our social media channels. Our campaign included, among others:

- a video statement of the EDPS Supervisor;
- a blogpost of the EDPS Supervisor;
- an infographic on data subjects' rights;
- a social media campaign raising awareness about data protection; and
- raising awareness on data protection amongst EUIs through collaborative work with other EUIs' communication channels, such as features in press and internal newsletters.

10.6.
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 plan to deliver another campaign, with a series of short videos, titled "Espresso with #teamEDPS".

In addition, we have also:

- revamped the layout of the EDPS' Vacancy Notices aiming at presenting our vacancies in a more candidate-friendly way;
- organised winter and summer campaigns promoting traineeships at the EDPS and focussing on attracting young talents;
- promoted regularly our Vacancy notices on the EDPS website; and
- cooperated with the EU Careers Staff Ambassadors to increase the visibility of the EDPS as an EU employer.

10.7. Collaborative Communication

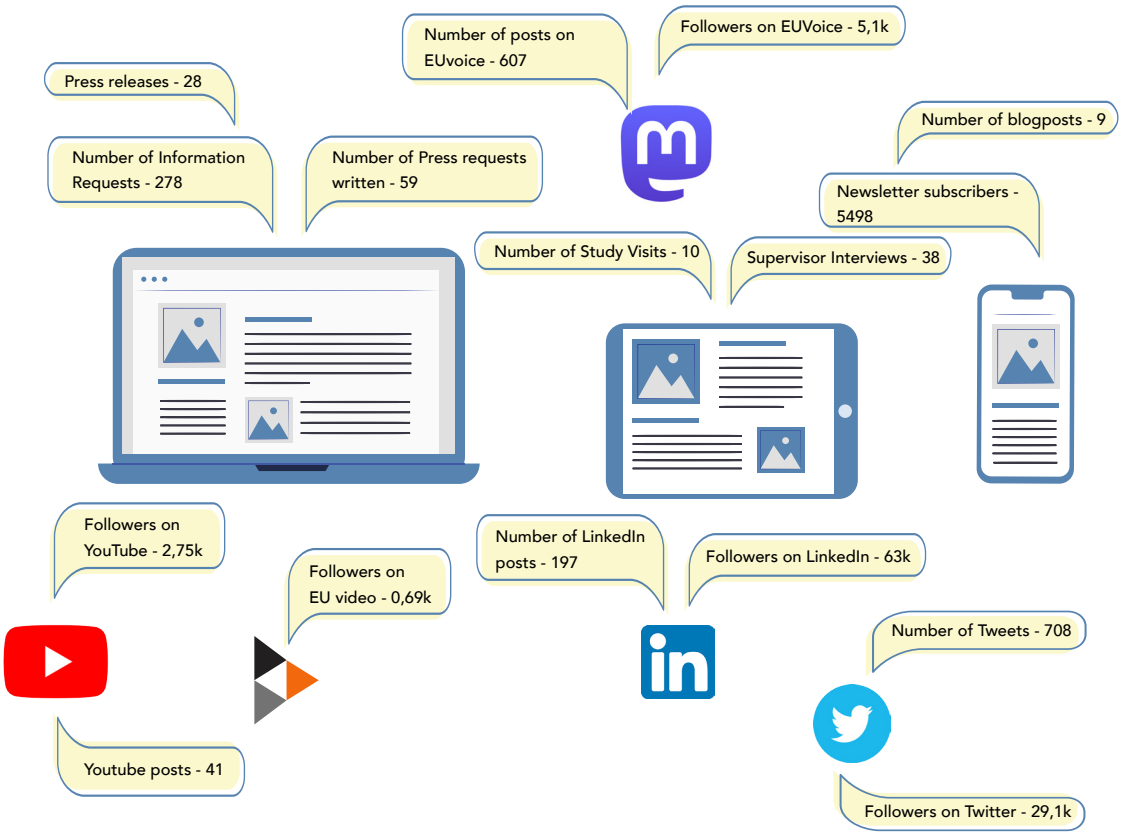
We have collaborated closely with other EU institutions, bodies, offices and agencies on communication tools and activities.

In relation to the launch of our alternative social media channels, EU Voice and EU Video, as a pilot project we worked on with the European Commission, we pursued our cooperation, to improve and promote its use amongst other EUIs as well, by highlighting the benefits of these platforms, such as explaining that they 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 pilot 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, for example, our automated machine eTranslation tool now available on our website.

In relation to communication activities, we joined forces with the European Union Agency for Cybersecurity (ENISA) and the European Commission to develop a campaign marking the 10th anniversary of the European Cybersecurity Month. We participated in a task force towards organising a campaign to contribute to its development and content dissemination. In parallel, we created our own content to highlight the data protection aspect of cybersecurity, focusing on two themes: phishing and ransomware. This effort, together with other initiatives, has been framed for the years to come in a Memorandum of Understanding between the EDPS and ENISA, establishing a strategic cooperation framework between us.

The EDPS' Communication activities in numbers



CHAPTER ELEVEN

The EDPS as an organisation

As an organisation we also have to manage our resources efficiently - such as our time, employees, finances - to be able to carry out our tasks as the EU institutions, bodies, offices and agencies' data protection authority.

With the opening of our EDPS Strasbourg office in June 2022, the creation of a dedicated legal service and other EDPS sectors, as well as the recruitment of data protection experts, the year 2022 saw our organisation evolve.

At the same time, we continued to make conscientious efforts in investing in our employees' well-being and their development through various initiatives, such as job-shadowing programmes.

A large part of our time was also dedicated to budget planning for EDPS activities.

11.1.
An evolving organisation

Identifying the need for our organisation to evolve to match our goals and vision, we have carried out a number of activities, such as expanding our organisation in Strasbourg, creating more EDPS sectors in specialised fields, and adapting our working conditions and some of our procedures to enhance the EDPS' efficiency.

11.1.1.

Expanding our outreach: EDPS Strasbourg office

To support one of the EDPS Strategy 2020-2024's objectives to reinforce its inter-institutional and international cooperation, we have established the EDPS liaison office in Strasbourg in June 2022, which will be officially inaugurated in March 2023. By setting up this office, we aim to provide additional support in the European Parliament's legislative process, including during the plenary sessions, fulfilling our role as advisor to the EU legislator on data protection matters.

11.2.

Organisational Changes

2022 saw some organisational changes at the EDPS.

The Head of the EDPS Secretariat

The EDPS' Human Resources Budget and Administration Unit (HRBA) supported the amendment of the EDPS Rules of Procedure, which entered into force on 14 November 2022, and the subsequent decision of the Supervisor to establish a new function of Head of the EDPS Secretariat at the level of a Secretary-General. For this new function, the HRBA unit started preparing the launch of a selection procedure beginning 2023.

A dedicated Legal Service

With the creation of a specific Legal Service function, we recognise the growing importance of high level in-house legal advice. With the stronger enforcement actions from the EDPS, comes an increased likelihood of judicial review of our actions. At the same time, our expertise is increasingly sought by the CJEU, as reflected in the number of hearing the EDPS has been invited to take part in. Lastly, the EDPS action for annulment concerning certain provisions of amended Europol Regulation illustrates the importance of Legal Service function as regards the capacity of the data protection authority to protect its independence.

The Governance and Internal Compliance Sector

Reflecting on the EDPS' organisational governance models and structures, a new sector, named Governance and Internal Compliance, was created within our organisation in early 2022. The aim of this sector is to create synergies between internal compliance and data protection obligations, transparency and access to documents, internal control coordination, records, archives and knowledge management, planning coordination, to enhance the EDPS' accountability and to support its compliance with applicable laws and obligations (see Chapter 12 and 13).

Other changes

Following a decision of the Supervisor, the HRBA unit prepared and implemented a number of organisation chart changes in the beginning of 2022. The changes involved the creation of two new operational sectors in the Supervision and Enforcement unit, a new Finance sector in the HRBA. In addition, HRBA ensured the selection of a new Head of Unit to fill the vacant position in the Technology and Privacy unit.

11.3.
Adapting working conditions

The changes in our working environment caused by the COVID-19 pandemic and the full-time teleworking regime called for a deep reflection on the adaptation of our working conditions. This reflection included factors like working time, hybrid working and telework from abroad, which lead to the adoption of new working time and hybrid working rules in May 2022. After a pilot phase of 1 year, an assessment will be carried out through staff consultation and the rules amended if necessary.

11.3.1.
Automating procedures

We pursued our efforts in further modernising and simplifying some Human Resources (HR) and administrative processes by automating some of these actions, such as the management of the probationary period of officials and contract agents by optimising the use of the HR management tool, Sysper. Using Sysper allows both employees and the employer of EUIs to consult their records, such as their personal file, appraisal and probation reports. By managing this process digitally we made this process more efficient for managers and staff involved.

11.4.
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 skills, job-shadowing programmes, and other initiatives.

11.4.1.
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 allow us to respond creatively to data protection challenges and find solutions that benefit society as a whole, especially the most vulnerable.

Recruiting data protection experts

To ensure that the EDPS and EDPB have the personnel and expertise to carry out the tasks assigned to them, there is a need for us to hire more data protection experts. In order to recruit this specialised workforce, we organised in 2022, with the support of the European Personnel Selection Office (EPSO), an administrator (AD) specialist open competition that resulted in the publication of a reserve list of 76 data protection experts, from which we started to recruit at the end of 2022.

In addition to recruiting data protection experts, the EDPS has hired various other profiles in the field of finance, communication, secretariat to support the increase of workload.

Our Traineeship programme

We continued to welcome 10 so-called Blue Book trainees, 8 for the EDPS and 2 for the EDPB, twice a year - once in October and once in March - as part of a Service Legal Agreement we have with the European Commission's Directorate-General for Education, Youth, Sport and Culture.

Our trainees take on an active role during their time at the EDPS and EDPB; they are given the space and support to lead projects on their own interest and knowledge. For example, in 2022, our two cohort of trainees created two podcasts, one on artificial intelligence and one on the EU Digital Identity Wallet.

11.4.2.
Employees' wellbeing and development

Job-shadowing

We have continued to offer a job-shadowing programme, adopted in December 2020.

Job-shadowing is a short-term exchange in which an EDPS member of staff is paired with another staff member of another EU institution, body, office or agency, to increase their respective understanding and awareness of the work, role and tasks done in the EU institutions involved.

For example, one staff member performed a job-shadowing at the European Commission, in the Communication unit of its Directorate-General of Human Resources, to learn more about the planning of events of different sizes.

Another noteworthy example, several HR members of staff performed a job-shadowing at the European Maritime Safety Agency, which is comparable to the size of the EDPS, to learn more about how they manage selection and recruitment, learning and development, wellbeing, and the management and application of guidelines related to staff's missions, when travelling for work for example.

In both instances, colleagues exchanged best practices, whilst also learning new skills to help inform their work as well as the EDPS' work as a whole.

EDPB Secondment Programme

In the same vein, we pursued the well-received EDPB Secondment Programme, which facilitates staff exchanges between the EDPS, the EDPB and the data protection authorities of the EU Member States and European Economic Area, so that they can each experience what it is like to work in different environments. We plan to assess this secondment programme in 2023.

Career development

In 2022, we continued to offer training courses via EU-LEARN to the EDPS staff. EU-LEARN is a platform for all employees of EUIs to sign up to training courses that contribute to enhancing and developing new skills related to their position or organisation. The platform includes training courses on a wide range of topics, from perfecting language skills, interpersonal skills and courses related to EUIs' core business activity, such as data protection. We also offered EDPS managers management-focused courses with the European School of Administration. Similar to previous years, external training sessions were also offered to our staff. When appropriate, and possible, colleagues take part in trainings organised outside of the EU institutions.

In addition to the training sessions that EDPS staff can participate in via EU-Learn, we pursed the organisation of "HRBA teasers", hosted and prepared by the EDPS' Human Resources, Budget and Administration Unit. HRBA teasers are short presentations covering procedures, tools and topics of interest for colleagues, such as how to use the HR tool of Sysper to encode annual leave, presences, or on IT tools and internal processes.

Coaching

In 2022, we continued to provide internal coaching and other activities for 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 18 individual sessions in full confidentiality in 2022. On top of this, our EDPS coach provided team coaching, with the aim of accompanying teams in improving their working relationships or setting priorities and goals in their work. Throughout 2022, the management team of the EDPS also benefited from four sessions of team coaching which were facilitated by our internal coach and an external coach.

Additionally, we also continued our co-development programme, a pilot project initiated in 2021, which is a type of group coaching in which participants learn from each other and consolidate their professional practice together. This co-development programme, initially organised for Heads of Sector and Heads of Activity as well as Deputy Heads of Unit was also extended to assistants and secretaries of the EDPS and the EDPB on a voluntary basis, in 2022. As a result, we facilitated sixteen sessions during which colleagues shared problems or preoccupations and supported each other in their professional practice.

EDPS Away Day

In the aftermath of the pandemic, we held an EDPS/EDPB staff away day with over 100 participants. This day was centred on collegiality: getting staff back together again after the pandemic, on-boarding newcomers and fostering cross team cooperation. The day included many activities and games in a lively and friendly atmosphere.

Wellbeing Activities

As an organisation that focuses on creating a positive impact in our society, one of our core values is to treat individuals, including our staff, with respect. To build a positive, respectful and safe working environment, we pursued a number of initiatives, including:

- guidelines to recognise, prevent and manage staff burnout;
- a review of the decision about the procedure relating to anti-harassment; and
- the appointment of confidential counsellors.

We believe that staff members who report higher levels of positivity, comfort and happiness at work are more likely to learn more effectively, be more creative, have better work-relationships, be more pro-social in their behaviour, feel more satisfied in their jobs and perform better. Therefore, encouraging well-being at work is of vital importance at the EDPS. To this end, a Well-being Coordinator was appointed at the EDPS to ensure that internal HR processes are in line with EDPS staff's well-being, and that colleagues have the knowledge and tools necessary to facilitate a high level of well-being at work, and whenever possible outside of work. The Well-being Coordinator role is normally held by a Human Resources' representative, as an approach focused on well-being immensely benefits recruitment and training, career planning, performance and talent management, engagement and recognition, leaving and retirement.

The wellbeing activities organised at the EDPS included for example:

EDPS/EDPB walks – Our internal coach, assisted by facilitators from other Units and the well-being coordinator, organised EDPS/EDPB walks. These walks, lasting half a day, enabled people to enhance team spirit and to get to know each other in an informal setting.

Office leisure activities – Our colleagues were encouraged to organise various leisure activities in small groups. The activities could include organising a book club, yoga classes, playing board games and solving puzzles, food tasting group or a language round table.

Our colleagues appreciated the introduction of these activities as they contributed to strengthening professional relationships and teamwork, which had an overall positive impact on our productivity. In addition, units that organised well-being activities often shared their experiences, which encouraged other units to partake in similar activities.

Staff Satisfaction Survey

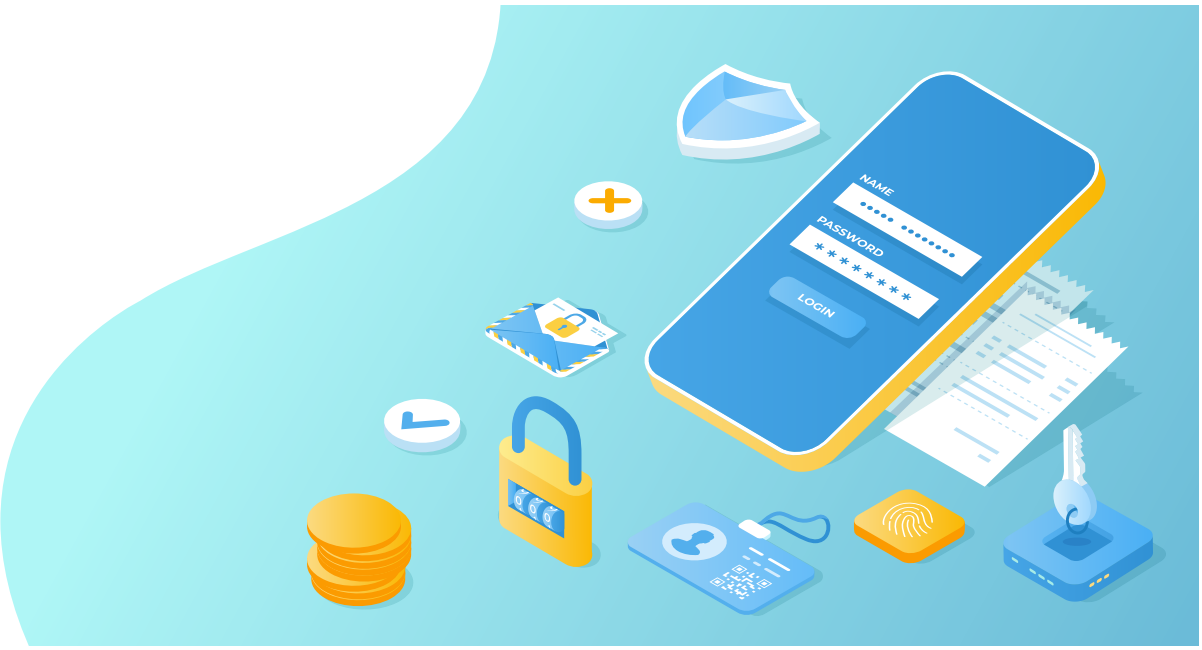
Staff satisfaction surveys are conducted bi-annually at the EDPS; the latest one was held in June 2022. These surveys allow us to gain an understanding of the evolution of our institution's environment.

Our latest survey focused on a number of topics including the EDPS as an employer, the work environment, job experience, inclusion and fairness and views on management. More than half of the EDPS staff - 66% - responded to the survey.

The results were mostly positive and confirmed a high level of satisfaction and staff engagement at the EDPS. The good relationship with colleagues, teamwork and willingness to put extra effort was highly rated amongst the responses submitted. We also received some valuable feedback and areas for improvement. As a follow-up, we proactively set up a task force in view to further evaluate the results of the survey, share its analysis and develop an action plan to address the identified issues.

11.5.
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.



11.5.1.
Budget

Budget execution

The 2022 EDPS operating budget amounted to EUR 20,266,000.

In addition, the EDPS received EUR 50,000 related to European Free Trade Association contribution.

Compared to the 2021 final budget, the operating budget increased by 4.12%.

In terms of budget execution, the commitment appropriations show an implementation rate of 98,23%. This positive trend was made possible due to an accurate monitoring of the budget forecast and sound planning of the EDPS' activities, such as events and conferences.

Budget preparation

The 2023 budget exercise, although very challenging in view of the annual inflation and unexpected high costs of living, was conducted successfully to meet the EDPS' planned priorities.

As was the case in previous budget exercises, the need to follow a rigorous approach regarding administrative expenditure and staffing of the European institutions in general has remained an imperative element in the preparation of the 2023 Draft Budget.

In the second EDPS' Draft Statement of Estimates for 2023, a proposed overall budget increase of 10.88%, and 9 additional establishment plan posts were requested. Despite our efforts produced in our second proposal, some cuts were performed by the European Commission and the Council.

The final approved budget foresees an increase of expenditure of 9.53% compared to 2022.

Budget monitoring

2022 followed the implementation of the Bluebell database. The EDPS uses Bluebell to establish and revise forecast for the budget based on data uploaded and updated by operational Units. Bluebell also allows to give a refined view of all budget lines by detailing them into actions (activities) and linking these actions with posting criteria in ABAC, the financial software used in the European Commission, so that the forecast can be compared in real time with the actual execution.

Overall, using this system has increased our efficiency in the preparation, monitoring and follow-up of the 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.

11.5.2.
Finance

The number of payment transactions (799) increased substantially in 2022 compared to 2020 and 2021. This can be explained due to a return to normal activities, following the COVID-19 pandemic. However, the number of transactions is still below the amount of transactions made in 2019 due to some activities being impacted by new ways of working, for example with the organisation of and participation online or hybrid meetings and events.

In terms of payment execution, there is a significant growth, even compared to 2019 (+23%). This increase is more marked if we look at the average payment amount by transaction: from 6.704€ in 2019 to 23.0766€ in 2022.

11.5.3.
Public Procurement

We hold public procurement procedures, depending on both the EDPS' and the EDPB's working programs and plans for the upcoming year. This may include the need for outsourcing certain activities, for example particular events, conferences, and other projects.

In this respect, part of the EDPS' HRBA Unit is to support both institutions in these procedures, by ensuring that these are conducted smoothly and that they comply with the budgetary principles laid down in the Financial Regulation for EUIs.

More specifically, the HRBA Unit focused on making 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 that favours healthy competition, fosters a qualitative collaboration between the EDPS and/or the EDPB and the contractor(s) in question.

Similar to previous years, the EDPS continued to participate in participating in large inter-institutional Framework Contracts, to achieve a higher degree of administrative efficiency. The most important inter-institutional framework contracts we are relying on are related to IT consultancy, interim services, office supplies and office furniture. In addition, we conducted one procedure for a framework contract in the communication field, as well as Call for Expressions of Interest to establish a List of Individual experts.

11.5.4.
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 the expenses and revenues are included in the correct financial year and that the annual accounts are complete and fairly represent the financial position and budget implementation of the EDPS.

The annual accounts cover the period from 1 January to 31 December 2022 and comprise the financial statements and the reports on the implementation of the budget. They 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.

11.5.5.

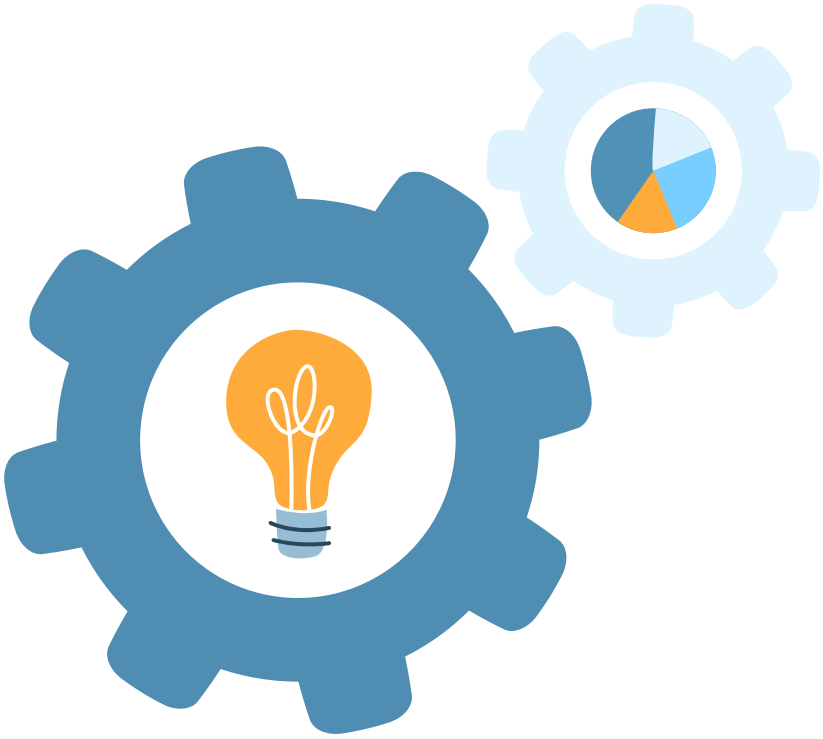
A new inventory management system

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.

11.5.6.

Managing missions more efficiently

In November 2022, the EDPS joined a PMO pilot project for the management of missions in a shared mode. Missions includes, for example, trips that staff make in the context of their work, to carry out their tasks. Using this Pilot Project means that staff going on mission can directly benefit from services offered by the PMO's mission experts; this is particularly relevant when it comes to declaring mission expenses and related reimbursements.



CHAPTER TWELVE

EDPS Data Protection Officer

The focus of the office of the Data Protection Officer (DPO) at the EDPS in 2022 was to enhance the EDPS' data protection compliance, whilst always keeping the role and mission of the EDPS in mind.

Considering the EDPS' role as the data protection authority (DPA) of the European institutions, bodies, offices and agencies (EUIs), as well as the high level of in-house expertise in the field, the DPO, together with the services in charge of personal data processing, continued to lead by example by raising and upholding the highest standards of data protection throughout 2022.

Moreover, as per the core action pillar of our EDPS Strategy 2020-2024, the EDPS continued to support EUIs to continue to lead by example in safeguarding digital rights and responsible data processing.

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 therefore continued to strengthen the EDPS' accountability by raising the standard of compliance of the ongoing and new personal data processing activities that the EDPS may need to carry out in their role as the DPA of EUIs, including seeking privacy and data protection friendly alternatives.

12.1.
Accountability

12.1.1.
Monitoring application of data protection rules

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

12.1.2.
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 EDPS supervision, IT, communication, administration and security.

12.1.3.
Updating data protection notices

We aimed to increase transparency and accessibility towards individuals and EDPS employees about how we process their personal data. We did this, and continue to do so, by publishing new and updated data protection notices that are more clear and comprehensive, in the most appropriate sections of the EDPS' website and intranet. Adding to this effort, we publish our data protection notices on the EDPS website, at times in English, French and German, to inform our viewers and readers on how their personal data will be processed, for example in the context of events organised by the EDPS or when visiting our website. Throughout 2022, we also regularly updated our data protection notices, for example in the context of EDPS events, webinars, video conference software, social media, human resources and administration.

12.1.4.
Ensuring compliance of services used by EDPS

We continued the process of scrutinising the services used by the EDPS in order to clarify the data protection responsibilities of contracting parties and adapting, where appropriate, contractual clauses. For example, when the EDPS uses external contractors for media services, event planning, communication tools. Likewise, the EDPS, as controller, continued its search and exploration of alternatives to large-scale providers, in the context of EU's "digital sovereignty", as per the EDPS Strategy 2020-2024.

12.1.5.
Assessing data protection risks

We assessed the risks to the fundamental rights and freedoms of individuals of new and ongoing processing activities, including on the need to carry out Data Protection Impact Assessments.

12.2.
Advising the EDPS

The DPO continued to advise and work closely with services in charge of processing personal data in order to ensure the EDPS' compliance with data protection law and principles. In particular, the DPO advised on the data protection compliance of new services that the EDPS is considering to use, for example in the fields of human resources, information security and communication. In many cases, a number of 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 for the EDPS; new and updated contracts with external service providers; and the review of certain internal rules and procedures.

12.3.
Enquires and complaints

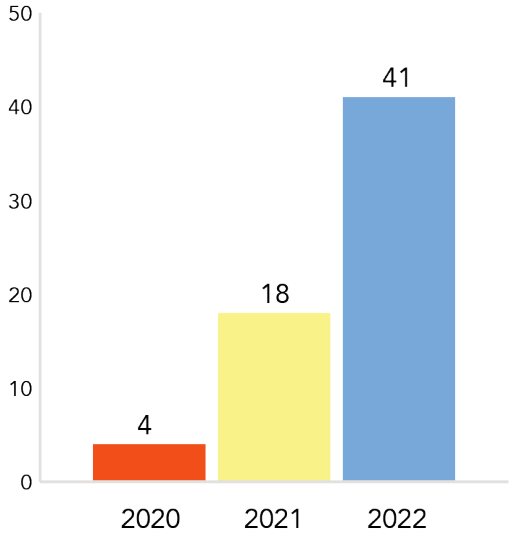
The number of enquiries, complaints and requests from individuals exercising their data protection rights received by the EDPS in 2022 increased in comparison to previous years.

Type of requests processed by the DPO of the EDPS in 2022

The DPO processed 23 access requests in 2022, while in 2021 the number of such requests was 6. An access request gives individuals the right to request a copy of their personal data that is being processed. In 2022, there were also 14 erasure requests, 3 information requests, 1 rectification request and 22 inadmissible requests. In certain cases, individuals exercised more than one data protection right, such as access and rectification requests. Access to personal data was provided in 5 cases, while in the other cases it was concluded that no personal data was processed by the EDPS.

With regards to erasure requests, only in one case personal data was processed by the EDPS. In that particular case, personal data of the applicant was erased partially. The individual was satisfied with the outcome.

Table 14: Evolution of data subject requests since 2020 (except inadmissible requests)



During 2022, the EDPS DPO received 6 complaints: 3 from EDPS staff and 3 from citizens. In 2 cases, personal data was processed directly by the EDPS, in 4 cases data was processed by processors. The complaints concerned the use of cloud services, consent collection, sharing of personal data with third parties, and the obligation to provide information.

Individuals may lodge a complaint with the EDPS, as a 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.

12.4.
Raising awareness about data protection

In 2022, 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 EDPS internal rules and procedures. 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 2022, which gave the opportunity to EDPS staff to employ both their expertise in data protection and their unique artistic talents. This competition was appreciated by our EDPS colleagues, as there was a variety of fascinating entries, for example songs, AI-created paintings and an AI-written story. This competition is one of the ways to reinforce collegiality between the EDPS staff, and to discuss data protection in a unique manner.

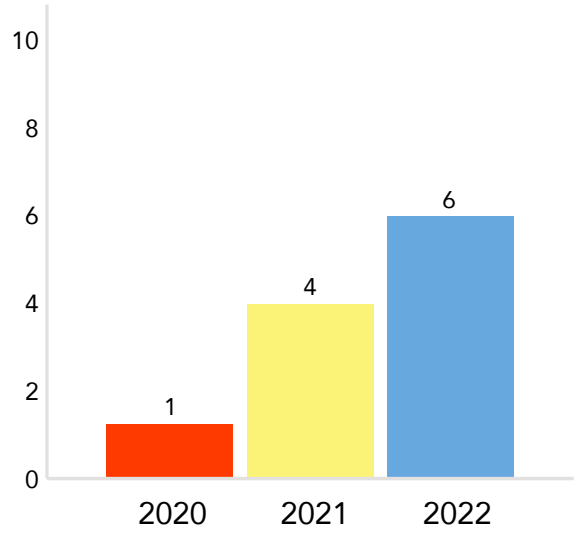
12.5.
Cooperation with other data protection officers

The DPO continued its collaboration with the DPOs of other EUIs, allowing for the valuable exchange of expertise and best practices in various formats, such as regular meetings and working groups on specific topics, which gather together DPOs and other experts. In addition, the DPO participated in the biannual meetings with the network of DPOs in June and December 2022.

The DPO also participated in the 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 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 topical subject matters were discussed, such as the use of AI by EUIs, the use of social media by EUIs and processing of health personal data, as well as fostering cooperation between the EUIs' DPOs and the EDPS.

Table 15: Evolution of the number of complaints received by the EDPS DPO since 2020



CHAPTER THIRTEEN

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 2022, the EDPS received 54 access to documents requests, which is an increase of over 80% in comparison to 2021. In 3 of these cases, we also received a confirmatory application. In all cases where documents could be identified, the requested documents were either fully or partially disclosed.

We remain fully committed to increasing the transparency and accountability of our work and aim to update our website, and our public register in particular, with relevant documents and information on a regular basis.

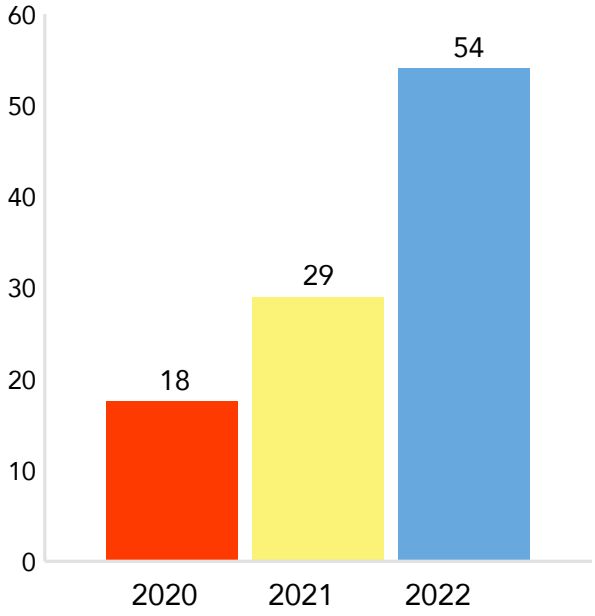


Table 16: Access to Documents requests since 2020

edps.europa.eu

Publications Office
of the European Union

EDPS