EDPS

EUROPEAN
DATA PROTECTION
SUPERVISOR

ANNUAL REPORT

EXECUTIVE SUMMARY '22

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

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 978-92-9242-810-5 ISSN 1831-0494 doi: 10.2804/293025 QT-AB-23-001-EN-C

PDF ISBN 978-92-9242-734-4 ISSN 1977-8333 doi: 10.2804/98849 QT-AB-23-001-EN-N

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 set 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 EUDPR), 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 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 supervisory 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.

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.

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**.

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.

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.

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.

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).

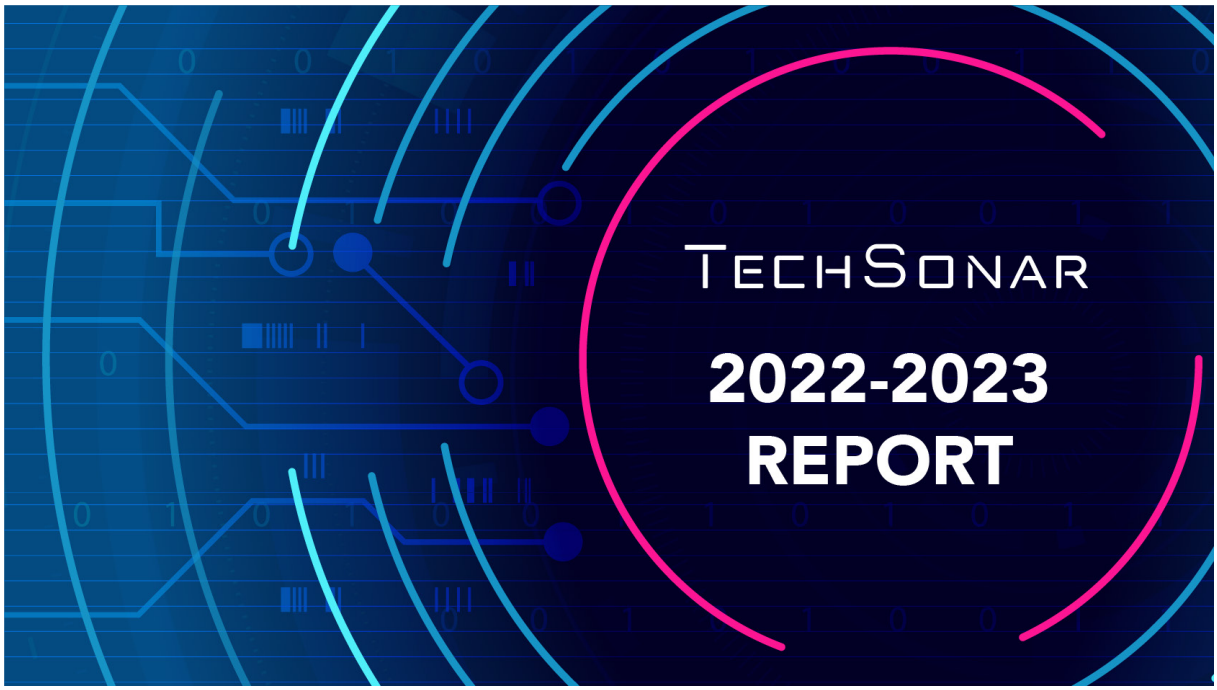
Our long-term vision for the future of data protection is clear: it is necessary to approach enforcement in a pan-European way to ensure real and consistent high level protection of individuals and to deliver the promise of the GDPR.

3.5.
Technology Monitoring & Foresight

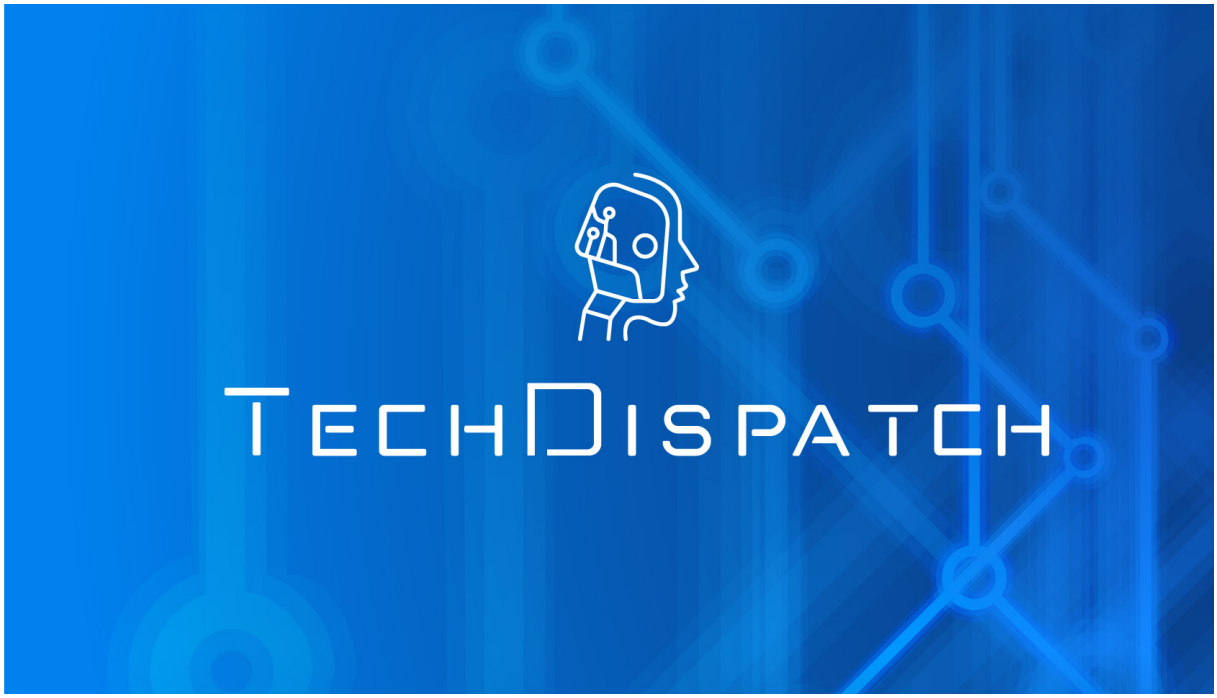
One of the three core pillars of the EDPS strategy for 2020-2024 is **foresight**, namely, our commitment to being a smart institution that takes the long-term view of trends in data protection and the legal, societal and technological context.

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.



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.

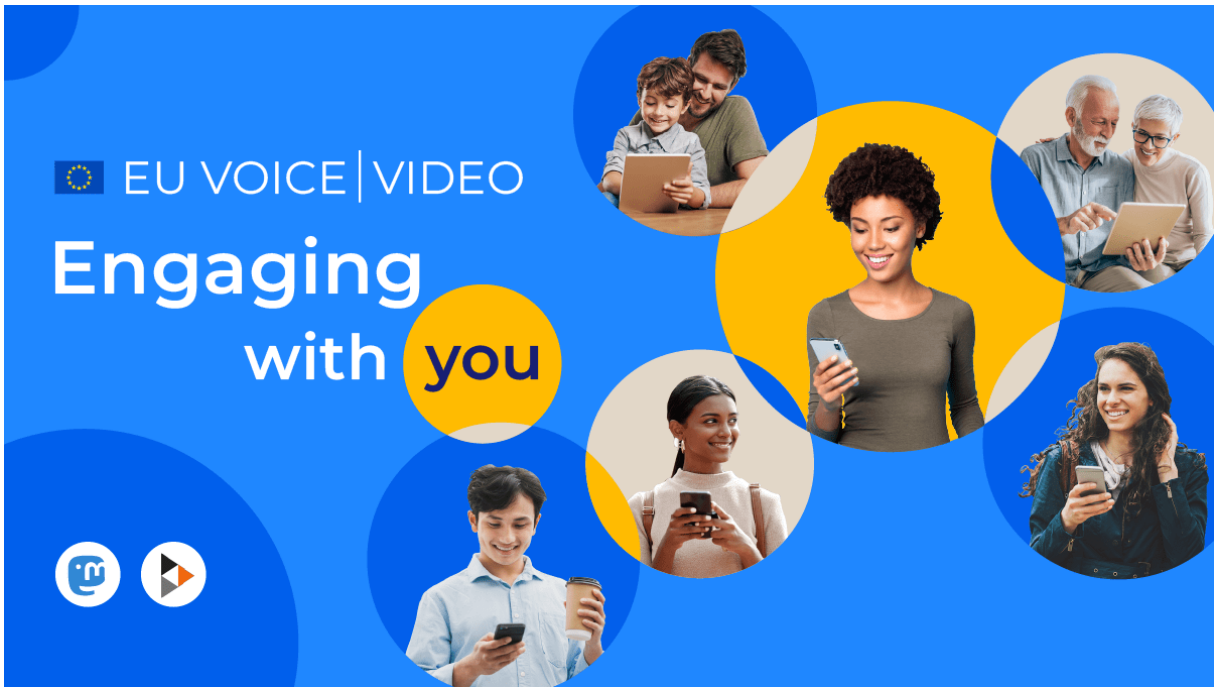


3.6.
Digital Innovation

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, for example. 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.

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%

edps.europa.eu

Publications Office
of the European Union

EDPS