



# MANDATE REVIEW 2020 2024

Further details about the EDPS can be found on our website [edps.europa.eu](https://edps.europa.eu)

The website also details a [subscription feature](#) to our newsletter.

Luxembourg: Publications Office of the European Union, 2025

© Design and photos: EDPS and European Union, 2025

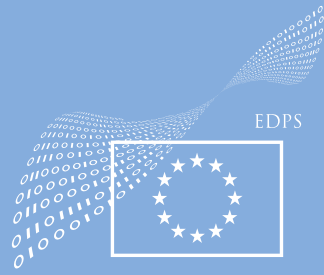
© European Union, 2024

Reproduction is authorised provided the source is acknowledged.

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

PRINT ISBN 978-92-9242-896-9 doi: 10.2804/4350762 QT-01-24-001-EN-C

PDF ISBN 978-92-9242-895-2 doi: 10.2804/2518798 QT-01-24-001-EN-N



EUROPEAN  
DATA PROTECTION  
SUPERVISOR

# EDPS MANDATE 2020 - 2024



# **Table of contents**

<b>Foreword</b>	<b>5</b>
<b>About the EDPS</b>	<b>7</b>
<b>CHAPTER ONE</b> <b>EDPS Strategy 2020–2024</b>	<b>9</b>
<b>CHAPTER TWO</b> <b>Key Performance Indicators 2020-2024</b>	<b>10</b>
<b>CHAPTER THREE</b> <b>Data protection in a global health crisis</b>	<b>13</b>
<b>CHAPTER FOUR</b> <b>Supervision &amp; Enforcement: protecting individuals' privacy</b>	<b>15</b>
<b>CHAPTER FIVE</b> <b>Policy &amp; Consultation: promoting a safer digital future for the EU</b>	<b>24</b>
<b>CHAPTER SIX</b> <b>Technology &amp; Privacy: anticipating the privacy challenges of tomorrow</b>	<b>30</b>
<b>CHAPTER SEVEN</b> <b>Artificial Intelligence: embracing opportunities, protecting people</b>	<b>40</b>
<b>CHAPTER EIGHT</b> <b>Setting global standards for data protection and promoting coherence across the EU</b>	<b>42</b>
<b>CHAPTER NINE</b> <b>Leading with independence and integrity</b>	<b>53</b>
<b>CHAPTER TEN</b> <b>Being recognised and recognisable as the EU institutions' data protection authority</b>	<b>56</b>
<b>CHAPTER ELEVEN</b> <b>Reshaping our organisation to meet data protection challenges</b>	<b>61</b>
<b>CHAPTER TWELVE</b> <b>Celebrating the EDPS 20<sup>th</sup> Anniversary</b>	<b>64</b>



## Foreword

The EDPS' 2020–2024 mandate has been synonymous with adaptability and resilience.

It started with a challenging year that none of us expected with a global pandemic, which not only dramatically changed the way we live and work, but also brought at the centre of public debate the role and nature of our fundamental rights, including the rights to privacy and data protection. My institution responded promptly to these new challenges by establishing an internal COVID-19 taskforce to coordinate and proactively undertake actions related to the interplay between privacy and the pandemic.

As supervisor of the EU institutions, bodies, offices and agencies (EUIs), we championed the highest standards of legal compliance necessary for their effectiveness, as proven by our audits, investigations, supervisory opinions, guidelines and training sessions. An efficient administration is an administration that respects the rule of law and acts on the basis of the law, not around it.

In the field of policy advice, we delivered a significant number of Opinions on legislative initiatives that have an impact on the protection of individuals' personal data, including the EU's new digital rule book and the European Health Data Space. Our Opinions are based on the conviction that data generated in Europe should be processed according to European values, to shape a safer digital future.



Monitoring technologies has also been a crucial aspect of our work. Our aim is to steer technological development in a privacy-enhanced way, to ensure that they embed data protection principles throughout their lifecycle. This ambition is coupled with our use of foresight techniques to anticipate the challenges and opportunities of the technology advancements that lie ahead, notably through our TechSonar and award-winning TechDispatch Reports.

Beyond the landscape of the EU institutions, the EDPS has always advocated for the elevation and coherence of data protection standards across the EU, as a member and provider of the European Data Protection Board, and globally through a variety of international fora. The EDPS takes leadership in the work of the Global Privacy Assembly, co-organises the International Organisations' workshop, for example.

Looking ahead, the EDPS has fostered much debate on the future of data protection, in particular with its conference on "The Future of Data Protection: Effective Enforcement in the Digital World", which focused on the progress needed on the future enforcement of the General Data Protection Regulation. The celebration of the EDPS' 20th anniversary, and in particular our

European Data Protection Summit: Rethinking Data in a Democratic Society, was also an opportunity to take stock of the work done in data

protection and the approach to take in the years and decades to come, especially when it comes to safeguarding our democratic society.

A handwritten signature in black ink, appearing to read 'Wojciech Wiewiórowski', with a stylized flourish at the end.

**Wojciech Wiewiórowski**

European Data Protection Supervisor



# About 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.

In addition, since the entry into force of Regulation (EU) 2024/1689 (AI Act) on 1 August 2024, the EDPS has taken up new roles and tasks in the supervision and enforcement of the applicable rules to AI systems developed or deployed by the EUIs.

## Our mission

Personal 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.



**“Together our goal is to protect people’s data”**  
**W. Wiewiórowski**

- **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.

## How we work

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

## Our powers

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

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

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

- [Europol](#) - the EU Agency for Law Enforcement Cooperation under Regulation (EU) 2016/794.
- [Eurojust](#) - the EU Agency for Criminal Justice Cooperation under Regulation (EU) 2018/1727.
- [EPPO](#) - the European Public Prosecutor's Office under Regulation (EU) 2017/1939.
- [Frontex](#) - the European Border and Coast Guard under Regulation (EU) 2019/1896.
- [eu-LISA - European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice](#) (Regulation (EU) 2018/1726).

In addition since the entry into force of the AI Act, Regulation (EU) 2024/1689 the EDPS also has the powers to act as the market surveillance authority and the notified body for AI systems developed or deployed by EUIs according to that regulation.

## CHAPTER ONE

# EDPS Strategy 2020–2024



In 2020, the EDPS laid out a comprehensive [strategy to shape a safer, fairer, and more sustainable digital Europe](#), in the spirit of collaboration and unity.

To achieve this, our institution set out three objectives guided by the following three pillars: **foresight**; **action** and **solidarity** that have signposted our actions across our three areas of expertise: **Supervision & Enforcement**; **Policy & Consultation**; **Technology & Privacy**.

Briefly, our Strategy sets out the following goals:

- **Foresight**

The EDPS will continue to monitor legal, social and technological advances around the world and engage with experts, specialists and data protection authorities to inform its work.

- **Action**

To strengthen the EDPS' supervision, enforcement and advisory roles, the EDPS will promote coherence in the activities of enforcement bodies in the EU and develop tools to assist the EU institutions, bodies, offices and agencies to maintain the highest standards in data protection.

- **Solidarity**


While promoting digital justice and privacy for all, the EDPS will also enforce responsible and sustainable data processing, to positively impact individuals and maximise societal benefits in a just and fair way.





CHAPTER TWO





# Key Performance Indicators 2020-2024



We use a number of key performance indicators (KPIs) to help us monitor our performance in light of the main objectives set out in the EDPS Strategy. This ensures that we are able to adjust our activities, if required, to increase the impact of our work and the effective use of resources. The KPI scoreboard below contains a brief description of each KPI and the results on 31 December of each year of the mandate.

KEY PERFORMANCE INDICATORS		Results 2023	Results 2022	Results 2021	Results 2020
KPI 1  Internal indicator	Number of cases, incl. publications, on technology monitoring and on promoting technologies to enhance privacy and data protection organised or co-organised by EDPS	20 cases	13 cases	16 cases	9 cases

KEY PERFORMANCE INDICATORS		Results 2023	Results 2022	Results 2021	Results 2020
<p>KPI 2</p>  <p>Internal &amp; External Indicator</p>	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8 activities	8 activities	8 activities	8 activities
<p>KPI 3</p>  <p>Internal Indicator</p>	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	36 cases	27 cases	17 cases	42 cases
<p>KPI 4</p>  <p>External Indicator</p>	Number of files for which the EDPS acted as a lead rapporteur, rapporteur, or a member of the drafting team in the context of the EDPB	20 files	21 files	23 cases	NA
<p>KPI 5</p>  <p>External Indicator</p>	Number of Article 42 opinions and joint EDPS-EDPB opinions issued in response to EC legislative consultation requests	56 Opinions	4 Joint Opinions 27 Opinions	17	6 Opinions 25 Formal Comments

KEY PERFORMANCE INDICATORS		Results 2023	Results 2022	Results 2021	Results 2020
KPI 6  External Indicator	Number of audits/visits carried out physically or remotely	9 audits/visits	4 audits + 1 visits	4 audits + 1 visit 43 EUs impacted	NA
KPI 7  External Indicator	Number of followers on the EDPS social media accounts	X: 29 413 LinkedIn: 71 238 EU Voice: 5 906 EU Video: 752 YouTube: 2 984 Total: 110 293	Twitter: 29.1k LinkedIn: 63k YouTube: 2.75k EU Voice: 5.1k EU Video: 0.69k	Twitter: 25 826 LinkedIn: 49 575 YouTube: 2 438	62 970 (LinkedIn: 38 400, Twitter: 22 493, YouTube: 2 077)
KPI 8  Internal Indicator	Occupancy rate of establishment plan	95.65%	86.9%	88%	71%
KPI 9  Internal Indicator	Budget implementation	96%	98.2%	86.12%	72.97

## CHAPTER THREE

# ***Data protection in a global health crisis***



The EDPS commenced its mandate during the COVID-19 health crisis. With the new realities brought by the pandemic in the EU institutions, as well as globally, our institution adapted its tasks.

From the outset, the EDPS emphasised the need for a pan-European approach when tackling the pandemic.

In 2020, the EDPS set up its internal [COVID-19 taskforce](#) to actively monitor and assess governmental and private responses to the outbreak, to provide the necessary tools and advice to EU institutions, and prepare for the future of data protection and privacy after the crisis.

With this task force, the EDPS took the leadership of assessing data protection standards of contact-tracing apps used to monitor the spread of the pandemic.

Notably, we issued [Guidelines on the use of manual contact tracing by EU institutions](#), distinguishing between the processing of health data of EUIs' staff members and non-staff members and advising EUIs on when and how to conduct a data protection impact assessment (DPIA) given the high sensitivity of the data and the privacy risks at stake.

Additionally, we published [Guidelines on body temperature checks](#) with the aim of counselling EU institutions who chose this course of action as part of their strategy for preventing the spread of the virus, given that the systematic check of the body temperature of staff and other visitors to EU institutions may constitute an interference with individuals' rights to private life and data protection. At the time, we stressed that just like any data processing operation, the obligations of data protection by design and by default should be applied to ensure that data collection in the context of body temperature checks is minimised.

Moreover, in response to mandatory consultations by the European Commission, the EDPS and the European Data Protection Board (EDPB) issued several Joint Opinions on the EU's Digital COVID Certificate Regulation. We issued recommendations to avoid direct or indirect discrimination of individuals, secondary and misuse of individuals' personal data by EU Member States, and to ensure that the principles of necessity, proportionality and effectiveness are upheld. The EDPS, as a member of the EDPB, also played an active role in developing a number of statements and guidelines on various data protection aspects of the COVID-19 pandemic response.

With our global outlook to data protection, we also championed the activities of the Global Privacy Assembly; an international platform composed of 130 data protection and privacy authorities from all over the world. In particular, we sponsored the Resolution on the Privacy and Data Protection Challenges arising from the COVID-19 Pandemic, with the aim of creating and sharing best practices.



## CHAPTER FOUR

# ***Supervision & Enforcement: protecting individuals' privacy***



The EDPS' Supervision and Enforcement Unit focuses on providing EU institutions, offices, bodies and agencies (EU institutions) with the appropriate guidance and necessary tools to uphold individuals' fundamental rights to privacy and data protection.

Our work in this area is multidimensional, focusing on the practical application of data protection law and principles in EU institutions' day-to-day work, as well as issuing guidance through Supervisory Opinions on important current affairs with an impact on data protection, and carrying out investigations and audits, as well as litigation in the Union courts.

### **1. Providing the necessary tools and resources to EU institutions**

Throughout the mandate, the EDPS took action to proactively develop tools for EU institutions to be world leaders in data protection.

#### **Advice through Supervisory Opinions and guidelines**

We provide practical advice to the EU institutions on subject matters they encounter in their line of work through the issuance of [Supervisory Opinions](#), which are targeted and tackle specific issues.

These include:

- data retention and storage limitation;
- controller-processor relationship, including joint controllership;
- the processing of special categories of data, including data concerning health and biometric data;
- the lawful restriction of individuals' data protection rights;
- the use of communication tools by EU institutions, including social media;
- the rules applicable to data protection officers;
- the transmission of personal data to recipients others than EU institutions.

We also issue [guidance](#) on different data protection issues of interest for EU institutions, including on:

- the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data;
- personal data and electronic communications in the EU institutions;
- internal rules restricting individuals' rights;
- different matters in the context of the Covid-19 crisis and, more recently, guidelines for EUIs using Generative AI.

## **The EDPS-DPO Network**

One of the other ways we ensure that we provide the necessary advice and tools to EU institutions is by advising and collaborating with their respective Data Protection Officers notably through the EDPS-DPO network held twice a year.

Each network meeting serves as a collaborative platform to foster dialogue, cooperation and knowledge sharing between the EDPS and the DPOs to ensure consistent compliance with the applicable data protection law, Regulation (EU) 2018/1725, within the EUIs.

The [EDPS-DPO Network meetings](#) are also an opportunity to take time to look at the concrete and practical application of data protection measures to day-to-day cases and problems EUIs may or have commonly encountered. This is done through the organisations of targeted workshops with the DPO Support Group, which is made up of volunteering DPOs who have hands-on experience.

Over the years, the network has helped tackle issues on and find new approaches to transfers of personal data, personal data breaches, the use of AI within the EUIs, data protection impact assessments.

## 2. Protecting individuals' rights

### Audits

As part of our supervisory work, we regularly conducted [data protection audits](#) to verify how data protection is applied in practice by EUIs. We ensure that we cover EUIs of all sizes in our annual audit planning.

The EDPS chooses to audit an EUI by taking into account a number of factors, including a risk analysis, whether special categories of data are processed, the time elapsed since the last audit or whether there has been an increase in the numbers of complaints. During an audit, we typically meet the staff members responsible for processing data at the EUI and request information or demonstrations.



We make continuous efforts to modernise our methods and procedures for audits based on clear rules, transparency, fairness and quality output. We are adapting our methods for audits according to international standards. In this regard, we have started working on adapting our policies and procedures to audit processing activities based on the use of new technologies, including artificial intelligence.

We acknowledge that for us to evolve as a modern, highly efficient organisation, we need to be more transparent in our processes and outcomes. In this regard, as part of the 20 Initiatives for the EDPS' 20th Anniversary, we have started to publish executive summaries of our audits and inspections reports.

### Investigations

Under Article 57(1)(f) of Regulation (EU) 2018/1725, the EDPS has the power to carry out [investigations](#). These investigations are triggered based on information received from third parties for example, complaints, press reports – or carried out on our own initiative. The aim of the investigation is to check whether an infringement of the applicable data protection rules has occurred and to establish its circumstances. If there was an infringement, the EDPS may decide to exercise corrective powers listed in Article 58(2) of the Regulation (EU) 2018/1725.

When EUIs do not comply with the data protection rules, [the EDPS can use corrective powers](#), such as:

- warn or admonish an EUI which is unlawfully or unfairly processing personal information;
- order an EUI to comply with requests to exercise individuals' rights (e.g. access to own data);
- impose a temporary or definitive ban on a particular data processing operation;
- impose an administrative fine on an EUI;
- refer a case to the Court of Justice of the European Union.

Throughout our mandate, our investigations have touched upon a variety of subject matters: assessing data protection risks of cloud services, the use of certain IT tools and their impact on data protection.

## 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 invest significant efforts in investigating [complaints](#) submitted by individuals who believe their data protection rights have not been respected by EUIs.

If we find that an EUI has infringed the data protection rules, we can exercise our corrective powers and issue a reprimand or order them to comply with a request from an individual to exercise their data protection rights, for example. 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.

## 3. Elevating data protection to a global standard: international transfers of personal data

One of the important topics we worked on during this mandate is transfers of personal data outside the EU/European Economic Area (EU/EEA).

Following the [landmark "Schrems II" judgement](#) delivered in June 2020 by the Court of Justice of the European Union invalidating the adequacy decision allowing the transfers of personal data between the EU/EEA and the United States of America (USA), the EDPS launched its strategy for EU institutions to comply with the ruling.

The [Strategy](#) aims to apply the Court of Justice's ruling on the importance of maintaining a high level of protection of personal data in particular in the context of international transfers. This strategic document identified short and medium-term actions to be carried out by EUIs. As a short-term compliance action, the EDPS ordered EUIs to map out and report all types of procedures carried out that involve transfers of personal data. Following through, as a medium term compliance action, the EDPS provided

guidance, compliance or enforcement actions for EUIs' procedures involving transfers of personal data to non-EU/EEA countries.

Work done by our institution in this domain led to the opening of two investigations: one on the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EUIs, and one regarding the use of Microsoft Office by the European Commission in May 2021.

The objective of the first investigation is to assess EUIs' compliance with the "Schrems II" Judgement when using cloud services provided by Amazon Web Services and Microsoft under the so-called "Cloud II contracts" when data is transferred to non-EU countries, in particular to the USA.

The objective of the second investigation into the use of Microsoft Office 365 was to verify the European Commission's compliance with the [Recommendations](#) previously issued by the EDPS on the use of Microsoft's products and services by EUIs, so that they can improve data protection compliance when negotiating contracts with their service providers.

In its investigation, the EDPS had found that the European Commission infringed several provisions of Regulation (EU) 2018/1725, the EU's data protection law for EUIs, including those on transfers of personal data outside the EEA. In its [decision of 8 March 2024](#), the EDPS ordered the European Commission to:

- suspend all data flows resulting from its use of Microsoft 365 to Microsoft and to its affiliates and sub-processors, located in countries outside the EU/EEA not covered by an adequacy decision ('suspension order'); and
- bring processing operations resulting from its use of Microsoft 365 into compliance by taking specified actions ('compliance order').

[The EDPS is currently reviewing the information provided to assess whether the European Commission has complied with the decision of March 2024](#). In the meantime, the Commission and Microsoft have lodged court proceedings in which they contest the EDPS decision (Cases T-262/24 and T-265/24).

Pursuing our efforts in this direction, the EDPS published its Model Administrative Arrangement in 2024 for transfers of personal data from EUIs to International Organisations to uphold compliance with EU data protection law, and thus to ensure that individuals' personal data is protected according to EU standards both inside and outside the EU/EEA. The Model places significance on data protection's core principles and puts in place the necessary safeguards to ensure a level of protection essentially equivalent to that guaranteed by EU legislation.

#### **4. Justice for all**

Fuelled by our belief that justice requires privacy to be safeguarded for everyone in all EU policies, our work in the area of Supervision and Enforcement is also dedicated to monitoring and supervising the Area of Freedom, Security and Justice, involving situations related to people on the move, EU and external borders, police cooperation and judicial cooperation in criminal matters. We have specific powers to supervise the bodies, offices and agencies processing personal data in this field.

This includes:

- [Europol](#) - the EU Agency for Law Enforcement Cooperation;
- [Eurojust](#) - the EU Agency for Criminal Justice Cooperation;
- [EPPO](#) - the European Public Prosecutor's Office;
- [Frontex](#) - the European Border and Coast Guard;
- [EUAA](#) - the European Union Agency for Asylum;
- [eu-LISA](#) - the European Union Agency for the Operational Management of Large Scale IT systems in the Area of Freedom, Security and Justice.



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 data protection legal framework in the AFSJ is still fragmented. Despite these discrepancies, we were 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.

A breakdown of our main activities during the mandate are detailed below.

As of 2021, we focused our supervisory activities over the bodies, offices and agencies in the Area of Freedom, Security and Justice around 8 pillar-actions.

- Preparing for the supervision of the interoperability framework.

- Reinforcing our cooperation with national data protection authorities either bilaterally or through our active participation in the Coordinated Supervisory Committee, in particular to coordinate supervisory actions. Amongst others, this resulted in the signing of a Working Arrangement with the Portuguese Data Protection Authority in the context of EPPO.
- 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.
- Supervising the efficient application of individuals' data protection rights, in particular in the context of our investigations of complaints against Europol.
- Scrutinising the processing of personal data by Frontex from debriefing reports in the context of joint operations. Supervising Frontex has revealed that the vague or excessively complex wording of the Agency's foundational legal framework is contributing to creating uncertainties regarding the exact scope of its 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 or of risk analysis.
- Assessing Europol's processing of biometric data and use of AI tools.
- Monitoring new ways of cooperation between Europol and EU Member States in carrying out operational analysis.
- Providing advice on the setting up of new systems to process operational personal data by Eurojust (war crime module) and EPPO (new environment to conduct operational analysis).

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

During the mandate, we took other important actions explained below.

## **Europol**

### *Europol's big data challenge*

During the mandate, the [EDPS finalised its investigation on Europol's big data challenge](#).

Initially launched in 2019, the investigation, pursued in several stages, first led the EDPS to admonish Europol in September 2020 for its continued storage of large volumes of data with no Data Subject Categorisation, posing risks to fundamental rights.

Despite some measures put in place to remediate the situation, Europol did not comply with our request to define an appropriate retention period to filter and to extract the personal data permitted, meaning that Europol was keeping data for longer than necessary, contrary to the principles of data minimisation and storage limitation. As such, we ordered the deletion of data concerning individuals with no established link to a criminal activity.

In practice, the EDPS imposed a 6-month retention period to filter and extract personal data. To this end, datasets older than 6 months that have undergone this Data Subject Categorisation were to be erased. At the time, the EDPS granted a 12-month period for Europol to comply with the Decision.

#### *Advocating for the rule of law and the EDPS' independence*

In 2022, [we took legal action as we consider that several provisions of the new Europol Regulation put the rule of law and the EDPS' independence under threat](#). We therefore requested that the Court of Justice of the European Union annuls two provisions of the amended Regulation.

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 the 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.

## **Eurojust**

Throughout the EDPS mandate, we carried out operational visits and regular meetings with Eurojust staff members to ensure their compliance with the latest data protection regulations.

## **European Public Prosecution Office**

The European Public Prosecutor's Office (EPPO) is the EU's first independent prosecution office that has the power to investigate, prosecute and bring to judgement large-scale, cross-border crimes against



the EU budget, such as fraud and corruption. The EDPS started preparations to supervise EPPO's activities since the EPPO Regulation came into force on 20 November 2017.

In its supervisory role at EPPO, the EDPS has been faced with a number of unparalleled questions due to EPPO's multi-layered legal framework and inhomogeneous structure. With its unprecedented scope, multiple references to national law, Regulation (EU) 2018/1725 and Regulation (EU) 2017/1939 (the EPPO Regulation) present a particular challenge for the supervision of personal data processing. Moreover, the unique investigative and judicial powers of EPPO in the area of criminal law may have profound impact on other fundamental rights.

## **European Border and Coast Guard Agency**

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

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. Frontex therefore breached the accountability principle as well as its obligations as a controller and the requirements of data protection by design and by default.

In addition to 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.

## CHAPTER FIVE

# ***Policy & Consultation: promoting a safer digital future for the EU***



As advisor to the EU's co-legislators—the European Commission, the European Parliament and the Council—on proposed legislation potentially impacting individuals' privacy rights to privacy and personal data, the EDPS has fulfilled its overarching objective to promote a safer digital future for the EU and the effective enforcement of data protection in a new regulatory landscape.

Over the course of the mandate, the EDPS has issued Opinions, Joint Opinions with the European Data Protection Board (EDPB), Formal Comments, as well as responded to informal consultations, on a variety of topics of concern for EU citizens, such as the EU's new digital package, health, finance, democracy, political advertising, the field of Justice and Home Affairs and more.

We issue Opinions at the request of the European Commission, which is legally obliged to seek our guidance on their legislative proposals that have an impact on personal data protection, or in the context of international agreements. In addition, the European Commission may also request a Joint Opinion with the European Data Protection Board (EDPB) if a legislative proposal is of particular importance for the protection of personal data. The EDPS also issues own-initiative Opinions on matters of specific significance. Furthermore, we issue Formal Comments that address the data protection implications of implementing and delegated acts in a more technical and targeted way.

In our role as advisor we have also developed practical [Guidance for co-legislators](#) on the main elements to consider when developing legislative proposals that imply the processing of personal data in order to ensure compliance with the Charter of Fundamental Rights, especially [Articles 7](#) and [8](#). This guidance builds on the EDPS' earlier toolkits for assessing the necessity and proportionality of measures impacting the fundamental right to data protection. The EDPS has also prepared a concept note on the 'essence'

of privacy and data protection rights – a critical concept in the legislative process, as any measure that compromises the essence of these rights is unlawful. Some of our notable work is detailed below.

## **The EU's new digital rulebook**

On 10 February 2021, we published Opinions on the European Commission's proposals for a Digital Services Act and a Digital Markets Act.

With these Opinions, both the EDPS and the EDPB aimed to assist the EU legislators to shape a digital future rooted in EU values, including the protection of individuals' fundamental rights, such as the right to data protection.

The [Digital Services Act](#) seeks to promote a transparent and safe online environment. In our Opinion, we recommend additional measures to better protect individuals when it comes to content moderation, online-targeted advertising and systems used by online platforms, such as social media and marketplaces.

Concerning the [Digital Markets Act](#), we welcomed the European Commission's proposal that seeks to promote fair and open digital markets and the fair processing of personal data by regulating large online platforms acting as gatekeepers. We highlighted the importance of fostering competitive digital markets, so that individuals have a wider choice of online platforms and services that they can use. To guarantee the successful implementation of the European Commission's Digital Services package, we called for a clear legal basis and structure for closer cooperation between the relevant oversight authorities, including data protection authorities (DPAs), consumer protection authorities and competition authorities.

In 2021 and 2022, we issued Joint Opinions with the European Data Protection Board on the [Data Governance Act \(DGA\)](#) and [the Data Act \(DA\)](#). The DGA aims to foster the availability of data by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. While recognising the legitimate objective of the DGA to improve the conditions for data sharing in the internal market, we provided several recommendations to ensure that the future DGA is fully in line with the EU personal data protection legislation. The Data Act, in turn, 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. To ensure protection of individuals, 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 concerned, 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.

## **Protecting democracy**

We issued an [Opinion on the Proposal for a Regulation on transparency and targeting for political advertising in January 2022](#), 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.

## European Health Data Space

We issued a [Joint Opinion with the EDPB on the EU Health Data Space](#) in which we advocated for strong protection of electronic health data in 2022.

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, without prejudice to grounds for transfer available in accordance with Chapter V of the GDPR. 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.

## **Combatting Child Sexual Abuse online**

Over the course of the mandate, the EDPS has worked on the [EU's proposal on child sexual abuse material](#), which aims to prevent and combat child sexual abuse online and offline by detecting the sharing of child sexual abuse material and grooming.

Whilst recognising the importance of this endeavour, we questioned the proposal's effectiveness, technical workability and the potential risk of the large-scale scanning of communication that could lead to constant surveillance.

In our view, the proposal fails to protect those who it intends to protect. Experts consider that detection measures cannot only be easily circumvented, but can also generate false positives. Furthermore, it is technically impossible to implement scanning for known or new content, and for the detection of grooming by a service provider without weakening end-to-end encryption and undermining users' privacy. Working on this file, [the EDPS also invited key experts and relevant stakeholders at a seminar held 23 October 2023](#) to discuss the proposal in more depth, and to inform our instead of its work in this area, allowing us to put recommendations at the service of people, and especially to protect the most vulnerable.

## **Financial Services**

We published an Opinion on the European Commission's proposed [Anti-Money Laundering legislative package \(AML\)](#) on 22 September 2021.

We welcomed the AML package and supported the general interest to fight money laundering and the financing of terrorism effectively. We appreciated the envisaged harmonisation of the AML/CFT framework through the enactment of a Regulation, as this would result in a more consistent application of the main rules by EU Member States. Moreover, we saw the harmonisation of the supervisory activities at EU level under the same European authority as a positive step, but called for a clear definition of the roles, from a data protection perspective, of all stakeholders involved in the supervision model.

We noted that the proposed AML package takes a risk-based approach to the screening of banks' clients in order to assess whether they may represent a money-laundering risk. While we appreciated the value of the risk-based approach underpinning the proposed legislative package, we considered that further clarifications are needed to minimise intrusion into individuals' privacy and to ensure full compliance with data protection rules.

On 23 August 2023, we published two Opinions: one on the proposal for a [Regulation on a Financial Data Access Framework](#) and one on the proposal for a [Regulation and Directive on payment services in the EU's internal market](#). Both proposals aim to foster the sharing of data to broaden the offer of financial services and products, whilst providing individuals or organisations control over the processing of their financial data. Given the highly sensitive personal data that may be shared, we provided several specific recommendations to ensure consistency with EU data protection law.

## Justice, home affairs and security

In addition to our supervisory role in the Area of Justice, Freedom and security, we also contributed to the development of the legislative framework in this field by responding to legislative consultations. In particular, we assisted the EU legislator and the European Commission by evaluating the necessity and proportionality of proposed measures in the light of the Charter of Fundamental Rights, applicable data protection legislation, and relevant case law of the Court of Justice of the EU.

In this context, we published Opinions on the legislative proposals for expanding the mandate of Europol, the EU Police Cooperation Code package, the Regulations on the collection and transfer of advance passenger information (API), on a number of international agreements on the exchange of personal data between Europol and Eurojust with the competent authorities of non-EU/EEA countries, and others. In addition, we issued series of Formal and Informal Comments on draft implementing and delegated acts related to the development and use of the EU large-scale IT systems (LSITS) in the area of Justice and Home Affairs and their interoperability framework.

The EDPS also contributed to the debate on the highly intrusive modern spyware by publishing Preliminary Remarks with a non-exhaustive list of specific recommendations as guarantees against unlawful use of spyware, such as strengthening of democratic oversight over surveillance measures, strict implementation of the EU legal framework on privacy and data protection, addressing the rule of law problems in the Union.

Moreover, we paid close attention to the challenging and complex discussion on the retention and access to electronic data by the law enforcement authorities. In this regard, the EDPS participated as observer in the 'High-Level Group on Access to Data for Effective Law Enforcement', jointly established by the Council and the European Commission, which has addressed a broad range of issues, such as retention of communication data, lawful interception and encryption.



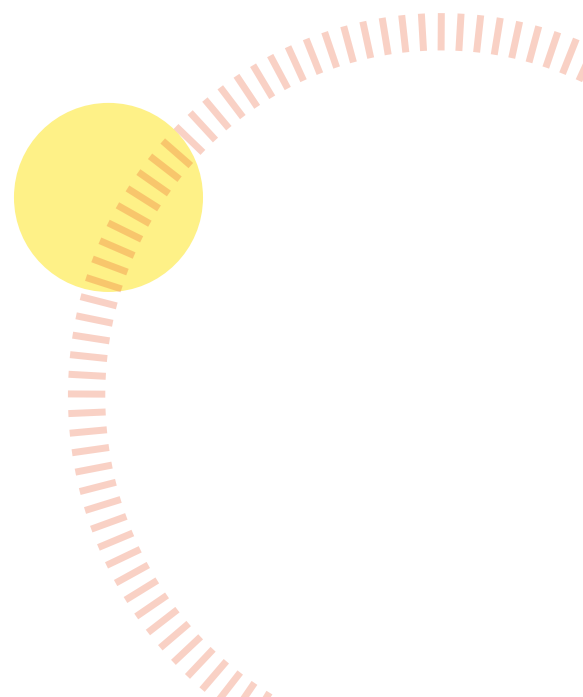
## **Participating in new EU regulatory bodies and expert groups**

As a member of the High Level Group (HLG) established under Article 40 of the Digital Markets Act, we actively participated, together with the EDPB, in the activities of this Group in order to promote a consistent regulatory approach across different regulatory instruments. We also provided a joint contribution on the information that gatekeepers should provide regarding consumer profiling techniques.

We also participated, alongside the EDPB, in the activities of the European Data Innovation Board (EDIB), an expert group established under Article 29 of the Data Governance Act (DGA) and chaired by the European Commission.

## **Towards a Digital Clearinghouse 2.0**

Parallel investigations by various authorities into the same practices of the same entities reveal the complexities inherent in applying different rules – such as data protection, consumer rights, and new laws such as the Digital Markets Act and the Digital Services Act – but also the importance of achieving a coherent regulatory approach. Simultaneous actions by various regulators highlight the potential for conflicts and inconsistencies when data-related practices are scrutinised from different legal perspectives. They also emphasise the critical need for enhanced dialogue, cooperation, and coordination amongst regulatory bodies to ensure a predictable and effective legal environment that places fundamental rights at the core. To this end, we have proposed ‘Digital Clearinghouse 2.0’ – a dedicated forum for interested regulators to identify emerging areas of cross-regulatory concern, facilitate coordination and to exchange knowledge, experiences and resources to enable effective cross-regulatory cooperation that is fit for the digital age.



## CHAPTER SIX

# ***Technology & Privacy: anticipating the privacy challenges of tomorrow***



The increase in digitalisation and automation in processing personal data has highlighted the importance the EDPS has always attached to understanding and assessing technology.

The EDPS has demonstrated its dedication to being a smart institution that focuses on long-term trends in data protection, taking into account legal, societal, and technological contexts.

We place strategic importance on integrating the technological dimension of data protection into our work. As a data protection supervisory authority, we need to identify and understand the state-of-the-art of technologies used to process personal data, to encourage the integration of data protection by design and data protection by default in the innovation process. At the same time, the EDPS must closely examine both the potential risks and opportunities offered by emerging technologies.

To this end, we have worked on multiple fronts.

### **a. Auditing IT systems**

The EDPS has played a pivotal role during this mandate in strengthening the security of IT systems managed by EU institutions (EUIs). Through regular audits conducted in accordance with international standards, the EDPS supports EUIs in preventing and addressing data breaches.

One of the EDPS' legal obligations is to regularly audit large-scale IT systems (LSITs), including the Schengen Information System (SIS), Eurodac, and the Visa Information System (VIS), to ensure compliance with relevant data protection legislation. With the upcoming deployment of new systems, such as the Entry-Exit System (EES) and the European Travel Information and Authorization System (ETIAS), as well



as the set up of the European Interoperability Framework, the EDPS's legal obligations in this area will continue to expand.

The data protection audits focusing on LSITs should follow international auditing standards. In the period 2022-2024, the EDPS further developed the methodology applied on these audits and will continue to do so. We apply a risk-based approach, assessing the effectiveness of controls in relation to the risks linked to the data subject. The ISO 27002 standard is used as a metric to evaluate security measures, providing a comprehensive set of guidelines for information security management.

Audits enable the EDPS to assess how data protection laws and principles are applied in practice within EUIs. These reviews also ensure that previous recommendations are put in place effectively. Amongst others, audits include specific topics IT systems security governance, data retention, security incident management, and personal data breach handling. Additionally, the EDPS assesses whether methodologies and practices used in system development, testing and operation adhere to the principles of data protection by design and by default, further to the principles of integrity and confidentiality.

## **Large Scale IT Systems Audits 2022-2024**

- *2022 Audit of Eurodac, Schengen Information System, and Visa Information System (VIS)*

In October 2022, the EDPS conducted an audit of the three systems managed by eu-LISA, the EU Agency managing large-scale IT systems in the Area of Freedom, Security and Justice. The audit focused on several critical areas and included a follow up of the recommendations from previous audits. The EDPS examined the methodologies and practices used for the secure development and testing of these systems, as well as the overall IT security governance of the systems. Additionally, the audit evaluated how security incidents and personal data breaches were managed within each system over a specified period, providing a comprehensive assessment of their security posture.

- *2023 Audit of the Schengen Information System (SIS)*

In December 2022, the EDPS conducted an audit of SIS. The audit assessed compliance with key information security controls, including information security policies, privileged access rights, technical vulnerability management, access management and logging, log retention and incident handling. Additionally, the audit evaluated eu-LISA's dactyloscopic (fingerprint) data processing within the SIS Automated Fingerprint Identification System (SIS AFIS) to ensure compliance with data protection requirements.

- *2023 Audit of the Internal Market Information System (IMI)*

In June 2023, the EDPS conducted an audit of the Internal Market Information System (IMI) focusing on security measures, data breach management, data retention, and monitoring and reporting mechanisms. Specifically, the EDPS assessed IMI's compliance with information security policies, access control, logging, and the management of technical vulnerabilities. The review also examined how the system adhered to regulations related to personal data breaches, retention periods, and monitoring and reporting obligations. The decision to conduct this audit was driven by the EDPS' mandate to oversee the application of the IMI Regulation in the processing of personal data.

- *2024 Audit of the Visa Information System (VIS)*

In December 2024 the EDPS audited the Visa Information System (VIS). The focus of the audit was on security measures and operational management. The audit also examined the implementation of key security controls, such as information security policies, access control, incident management, and network security. Furthermore, the EDPS assessed compliance with technical implementation requirements, record-keeping obligations, and data retention rules for the central VIS.

- *Follow up Audits*

In 2024, the EDPS introduced a more structured approach by separating general audits of Large-Scale IT Systems (LSITs) from follow-up audits. This change allowed for a more specific perspective in monitoring the application by controllers of recommendations from previous audit reports. As part of this approach, follow-up audit activities were completed for the VIS, SIS, and Eurodac systems, while a follow-up review was initiated for the Internal Market Information System (IMI).



These audits are a critical tool for the EDPS to ensure that EUIs adhere to data protection principles, maintain the confidentiality and integrity of personal data, and continuously improve the security of their IT systems.

The EDPS will continue to conduct regular audits and follow up audits to the LSITs to ensure compliance with the law.

## **EUIs Website Audits**

For many citizens, EUIs' websites are one of the most visible ways to keep up to date with their activities, providing users with a gateway to a vast array of information and services, making them an essential tool for engaging with the EU.

However, the growing number, size, and complexity of these websites, often rely on embedded third-party components such as maps, videos, and audio, creating new privacy and data protection challenges. In response to these challenges, the EDPS has conducted comprehensive audits on 28 EUIs' websites. These audits focused on key areas of concern, including security vulnerabilities, the presence of third-party content, the use of cookies and other tracking techniques for advertising and profiling purposes, and the accuracy and completeness of privacy notices, cookie policies and cookie banners.

## **EUIs' Mobile Application Audits**

In a similar way, as EUIs continue to expand their digital presence, mobile applications have become a tool for providing their staff and citizens with convenient access to information and services. However, with the increasing use of mobile apps comes a growing responsibility to ensure the protection of personal data. The mobile applications' ecosystem is far more complex than the one of web applications, for example EUIs' mobile users are not administrator of their own devices and discovering parties processing mobile app data is very difficult. The EDPS audited four mobile applications offered by EUIs to check their compliance with the legal requirements set in Regulation (EU) 2018/1725.

### **b. Protecting people affected by data breaches in EUIs' systems**

The EDPS is responsible for managing notifications of personal data breaches in accordance with Articles 34 and 35 of Regulation (EU) 2018/1725. This involves verifying controllers' assessments of the risks posed by such breaches to individuals' rights and freedoms, as well as determining the necessity of communicating these breaches to affected individuals. By handling personal data breaches, the EDPS not only ensures compliance but also promotes the continuous improvement of data protection practices across EU institutions.

Since the EU Data Protection Regulation (EUDPR) came into force in 2018, the EDPS has received nearly 500 personal data breach notifications from EUIs. Over the years, the number of breaches has risen, with a noticeable increase in their severity.

To address the growing number of notifications, in 2022 the EDPS implemented a more structured approach to manage data breach notifications more effectively. This proactive approach strengthened oversight and improved the efficiency of data breach handling.

We note that there is a need for increased investigations and audits concerning critical personal data breaches that pose a high risk to individuals. Following the completion of a pre-investigation in 2024, the EDPS will further develop its methods and supervisory activities. This will lay the groundwork for swift action in response to critical incidents and ensure that data controllers implement effective mitigation measures.

By the end of 2024, the EDPS has made significant progress in streamlining the notification process and establishing a more consistent supervisory mechanism. This development represents a major step forward in enhancing the EDPS' capacity to oversee personal data breach management across EU institutions.

## **Raising the awareness on personal data breaches**

Regulation (EU) 2018/1725 appoints the EDPS as a guardian of people's fundamental rights when information systems under EUIs' responsibility undergo data breaches. We verify the controllers' assessment of the risks posed by such breaches to individuals' rights and freedoms and the necessity of communicating these breaches to those individuals.



Our priority, however, remains to help EUIs to prevent personal data breaches. In this regard, it is crucial to raise awareness among EUIs on how to manage such incidents effectively. In recent years, the EDPS has organized several training sessions and workshops focused on personal data breach management.

In 2024, the EDPS launched an awareness campaign for EUIs that have never notified a personal data breach, with the aim to gain insights into how EUIs handle personal data breaches and providing guidance on improving their internal procedures.

We identified several key findings and provided tailored recommendations to EUIs to address the observed challenges. These recommendations focused on enhancing compliance, supporting organisational development, and improving the protection of data subjects' rights and freedoms. To ensure long-term improvements, the EDPS proposed forward-looking measures aimed to the DPOs: enhancing their personal data breach management process, supporting the establishment of risk management frameworks and improving their allocation of resources for compliance efforts.

As part of this initiative, the EDPS developed a new tool for self-assessment that may be further used by other competent authorities or even further extended to other data protection areas with significant benefits.

Additionally, we collaborated with ENISA, co-organised a table-top cyber exercise titled “Personal dATa bReach awareness In Cybersecurity Incident hAndling” (PATRICIA). The objective was to raise awareness about personal data breaches and foster collaboration among EUI staff to ensure the effective mitigation of risks to individuals through a practical initiative. The exercise brought together IT Managers, Data Protection Officers (DPOs), and Security Officers (LISO, LCO) from six EUIs, all of whom are responsible for managing cyber incidents involving a personal data breach. The exercise led to four key findings, which were documented in an after-action report shared with participants to support the improvement of current activities and procedures. Given the benefits for participants, the EDPS is considering repeating this exercise in the future.

## **Improving privacy of European Institutions’ websites**

During 2024, the EDPS started the Website Compliance Awareness Campaign to help EUIs identify potential compliance issues on their websites. The campaign aims to support controllers in fulfilling their accountability obligations under the Data Protection Regulation for EUIs and the ePrivacy Directive.

The EDPS used its Website Evidence Collector (WEC) tool to scan 73 websites every 6 months, starting in October/November 2024. The WEC provides a factual report on each website, highlighting potential issues and areas of improvement from a data protection perspective.

The campaign, planned as a pilot exercise, consists of three waves (autumn 2024, spring 2025 and autumn 2025), with each EUI receiving a notification and report after each wave. The EDPS will use the information collected to calculate aggregated statistics with indicators that signal potential issues with the EUDPR and the ePrivacy Directive.

The campaign will end in autumn 2025. If successful, the EDPS may scale it up to cover all websites under EUIs’ responsibility (around 1.300).

## **Technology monitoring and foresight**

The EDPS has the duty to monitor future data protection developments and in particular how technology evolves, to be ready to face future challenges.

At the EDPS, we do not see technology monitoring activities as isolated exercises. Most of them are interlinked so that our knowledge and understanding of technological developments is built up in successive layers and, so that we can add the most added value to our policy making and supervisory activities. This holistic view is implemented through the combination of several deliverables and activities described below.

## TechSonar: all eyes on the technologies that shape our future

Most notable, in 2021, [we launched TechSonar](#), our foresight project to anticipate emerging technological trends, the value and the risks they bring to individuals and society, instead of reacting to these trends, once the technology is widely deployed.

The main aim of this initiative is to better understand future developments in the technology sector from a privacy and data protection perspective. Based on the collective intelligence of the EDPS staff, we aim to contribute to the wider debate on foresight within and outside the EUIs.

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.

[TechSonar 2023-2024](#) explored large language models, the digital identity wallet, the internet of behaviours, extended reality and deep-fake detection.

[TechSonar 2025](#) focuses on different AI technologies, including retrieval-augmented generation, on-device artificial intelligence, multimodal artificial intelligence, machine-learning; and neuro-symbolic artificial intelligence.

For these reports, we provide a summary of each technology, its impact on our day-to-day lives, assess its possible effects on individuals' privacy now and in the future and provide a list of recommended readings for those willing to dig deeper into the topic.

TechSonar won the Global Privacy and Data Protection 2023 Award in the category Innovation.



## TechDispatch: assessing the impacts of technologies on privacy

Whereas TechSonar is a first and brief contact with certain technologies, [TechDispatch](#) offers a deeper and closer look to specific technologies that may have a noticeable impact on privacy and data protection.

Launched in 2019, our team of in-house Technology and Privacy experts have brought their insights on various emerging technologies over the years, such as neurodata, explainable artificial intelligence, federated social media platforms, and quantum computing, to name a few examples.

TechDispatches offer factual descriptions, preliminary assessments on privacy and data protection impact, and recommended readings. Some TechDispatch issues might touch upon technologies included in TechSonar (e.g. central bank digital currency) while others might not (e.g. Facial Emotion Recognition).



Our work on [TechDispatch](#) received the [Global Privacy and Data Protection 2021 Award](#) in the category of “[Education and Public Awareness](#)”, proving its international relevance and pertinence to the data protection community.

## The Internet Privacy Engineering Network: cooperating for privacy-engineered solutions

Initiated in 2014, the EDPS has kept up its regular [IPEN workshops and webinars](#) with developers and data experts in the EU and beyond to promote and advance the state-of-the-art of privacy engineering.

IPEN events gather public authorities, academia, open source projects and private businesses in an effort to find engineering solutions to privacy challenges. IPEN events are also one of the EDPS means to foster the discussion on relevant technological trends. We use what we learn from this discussion in the rest of our Tech Monitoring deliverables.

Since 2020, each IPEN event has focused on a specific topic, ranging from synthetic data to explainable Artificial Intelligence. However, depending on technological developments, IPEN could be dedicated to more than one topic or technology.

Over the mandate, the EDPS has hosted, but also collaborated with stakeholders to bring about IPEN events on the human oversight of automated decision-making, explainable artificial intelligence, central bank digital currency, to name a few examples.

Since 2016, the EDPS and ENISA have coordinated the organization of their IPEN event and Annual Privacy Forum respectively. This coordination has brought benefits to both institutions, leveraging existing synergies and avoiding potential topic or speaker overlaps.

## **Contributing to the global effort towards data protection by design and by default**

The EDPS has continued its tradition of contributing to the overall tech-savvy capacity of the EDPB by offering its own specific expertise and professionalism. Such capacity is a strategic and necessary asset of the EDPB in all its advisory and supervisory tasks, in a context where the digital component grows in relevance and complexity.

The EDPS' work on technology monitoring and foresight has recently been valued in international contexts such as the [International Working Group on Data Protection in Technology \(IWGDPT\)](#), also known as Berlin Group, with a view to identifying future topics for its recommendations and guidelines. In these years we have been among the most active contributors in the Group, recently leading the drafting of a paper on Central Bank Digital Currency issues. In 2024, we organised a successful meeting of the IWGDPT in Brussels, featuring a record participation and interesting discussions with a view to issue guidance papers such as the one on Neurotechnologies.

### **c. Fostering digital transformation that puts people first**

As part of our aim to minimise our reliance on monopoly providers of communications and software services to avoid detrimental lock-in, the EDPS progressed in its exploration and deployment of free and open source software and solutions.

At the same time, we strive to offer our employees a more modern workplace to support their work, while upholding the values of the EDPS in terms of data protection compliance.

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

As such, during this mandate, the EDPS advanced digital transformation and innovation within the EU's data protection framework by launching pilot open-source solutions on decentralised platforms, and automated compliance tools.



In particular, in February 2023, [the EDPS started piloting the use of the Open Source Software Nextcloud and Collabora Online](#) to share files, send messages, make video calls, and allow collaborative drafting, in a secured cloud environment.

We believe that these types of tools offer data-protection alternatives to commonly used large-scale cloud services providers. These open source platforms do not contain any advertisements and there is no profiling of individuals using them. The aim was thus to give individuals control over their personal data.

Similarly, the EDPS launched two alternative, decentralised social media platforms pilots, EU Voice and EU Video. With this initiative, the EDPS contributed to the EU's strategy for data and digital sovereignty to foster independence in the digital world. EU Voice allows users to interact with the public by sharing short texts, images and videos; whilst EU Video is for sharing, uploading, commenting videos and podcasts.

The pilot project, initially launched for a year, was prolonged for a second year. However, despite our efforts, we did not obtain adequate resources and were unable to secure a new ownership among other EU institutions to maintain EU Voice and EU Video service operations at the high standards that EU institutions deserve.

#### **d. Collaboration in technological matters**

The EDPS fosters collaborations in technological matters with other organisations, including EUIs, other data protection authorities and academia. The activities reported above include co-operations with these organisations. We mention a couple of examples here.

In 2023 the EDPS has signed a [Memorandum of Understanding \(MoU\) with ENISA](#) that focuses on synergies in cybersecurity and personal data protection. The objective includes sharing best practices and collaborating in events, publications and initiatives. The cooperation between ENISA Annual Privacy Forum and the EDPS IPEN initiative, or the PATRICIA personal data breach exercise are example of actions under the MoU.

The EDPS has also signed an [MoU with the Spanish data protection authority \(AEPD\)](#). The AEPD has co-authored with us many technology monitoring papers, which include the TechDispatch on Neurodata and the joint paper on 10 misunderstandings related to anonymisation.

These forms of collaboration, which we are keen to continue and reinforce, are key to a coherent approach to privacy and data protection and to leveraging common expertise for people's benefit.

## CHAPTER SEVEN

# ***Artificial Intelligence: embracing opportunities, protecting people***



Since the [entry into force of the AI Act on 1 August 2024](#), the EDPS is now the competent market surveillance authority for the supervision of AI systems developed or deployed by European institutions, bodies and agencies. The AI Act also designates the EDPS as notified body for conformity assessments of certain high-risk AI systems. Furthermore, the EDPS is competent to investigate complaints by individuals against such AI systems or also to fine the EUIs if they do not comply with the AI Act. The EDPS dedicated much time and effort to prepare its strategy for the use, development and deployment of AI by the EUIs and initiated organisational and procedural preparations for an effective enforcement of the AI Act in the future.

The [EDPS' AI Preparedness Strategy](#) is composed of three pillars: **governance** meaning relationships with supervised entities, governing bodies in the AI Act and international stakeholders, establishing a framework and culture for AI **risk management** in EUIs and its new role as a **market surveillance authority and notified body**.

With regard to **governance**, the EDPS proposed as a best practice the creation of the function of AI Correspondents—a function not explicitly required by the AI Act—in all EUIs as well as the creation of a network of all AI Correspondents. This network allows close cooperation with the EDPS and aligning and sharing expertise with the other EUIs. Furthermore, the EDPS coordinates with key stakeholders for the implementation of the AI Act notably the Commission's AI Office and participates in the AI Board and its sub-groups as an observer.

With regard to its **role as the AI supervisor of the EUIs**, the EDPS will prepare internal procedures to ensure compliance, handle complaints, or sanction infringing AI systems.



Prior to the entry into force, to ensure the EDPS' preparedness, and, by extension, EUIs, we contributed, together with the EDPB to the development of the AI Act, making multiple recommendations for its appropriate use, to avoid interference with individuals' fundamental rights to privacy and data protection. Following this direction, the EDPS and the EDPB successfully called for a ban on the general use of automated recognition of human features in publicly accessible spaces as this could lead to discrimination, and advocated for the AI Act to follow and apply the data protection principles already laid out in the EU's data protection laws.

Following AI's development and use in the EUIs, the EDPS has also developed guidelines on Generative AI to help them comply with EU data protection law when using or developing generative AI, covering many possible scenarios involving the use of these tools, to provide enduring advice to EU institutions so that they can protect individuals' personal information and privacy.

## CHAPTER EIGHT

# ***Setting global standards for data protection and promoting coherence across the EU***



One of our top priorities during the mandate is to channel cohesive and consistent data protection practices across the EU and European Economic Area, and to elevate such data protection standards at global level.

To achieve this, we continued to build the capacity of the European Data Protection Board, both as a member and as a provider of its secretariat, to ensure that the GDPR is a recognised model for democracies around the world. and contribute to various international fora.

### **General Data Protection Regulation enforcement**

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

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

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

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

## Cooperation in the European Data Protection Board

As well as providing its Secretariat, including its logistical resources, the EDPS is also a full member of the European Data Protection Board (EDPB). The EDPB is an independent European body that the General Data Protection Regulation and the Law Enforcement Directive are applied consistently and ensures cooperation, including on enforcement.

The EDPB is composed of the heads of the national data protection authorities (Supervisory Authorities) of the countries in the European Economic Area, as well as the European Data Protection Supervisor (EDPS).

To this end, we have participated and lead many initiatives; some of which are exemplified below.

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

### Initiatives carried out in 2023

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

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

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

The EDPS also provided significant input for the Guidelines 01/2023 on Article 37 Law Enforcement Directive; the Contribution of the EDPB to the report on the application of the GDPR under Article 97

or for the EDPB best practices for the organisation of EDPB Plenary meetings. Lastly, we supported the creation of a taskforce on the interplay between data protection, competition and consumer protection, acting as its co-coordinator.

## **Coordinated Enforcement Framework: working together with other enforcers**

The EDPS has participated in two coordinated enforcement actions, which is part of the EDPB's [Coordinated Enforcement Framework](#) (CEF) to streamline enforcement actions and cooperation amongst the data protection authorities of the EU/EEA.

The first coordinated enforcement action that the EDPS participated in 2022 focused on the use of cloud services by the public sector, in particular regarding the controller-processor relationship and when international transfers are involved. This exercise played an important role in ensuring that cloud-based services are fully compatible with EU data protection laws.

In March 2023, our institution took part in the Coordinated Enforcement Action on the role and tasks of data protection officers in the EU institutions, to help them bridge the gap between EU data protection law and its practical application.

## **EDPB Opinions on adequacy decisions**

In 2021, our work with the EDPB involved Opinions on adequacy decisions; some examples are listed below. An "adequacy decision" is a decision adopted by the European Commission on the basis of Article 45 of the GDPR, which establishes that a non-EU/EEA country—a country not directly bound by the GDPR or an international organisation—provides an equivalent level of protection for personal data as the EU does. The effect of an adequacy decision is that personal data may flow from the EU/EEA to that non-EU/EEA country without any further data protection safeguards being necessary.

[EDPB Opinion 14/2021 on the assessment of the adequate protection of personal data in the United Kingdom according to the GDPR](#). In this Opinion, challenges addressed include the monitoring of the evolution of the UK legal system on data protection as a whole. The UK government indicated its intention to develop separate and independent policies in the field of data protection with a possible will to diverge from EU data protection law. This possible future divergence might create risks for the maintenance of the level of protection provided to personal data transferred outside the EU. Therefore, the European Commission is invited to closely monitor such evolutions from the entry into force of its adequacy decision, and to take necessary actions including, amending and/or suspending the decision if necessary.

[EDPB Opinion 15/2021 on the assessment of the adequate protection of personal data in the United Kingdom according to the Law Enforcement Directive \(LED\)](#). In this Opinion, the EDPB recommended that the European Commission considers amending the adequacy decision to introduce specific safeguards for personal data transferred from the EU, and/or to suspend the adequacy decision in case the essentially equivalent level of protection of personal data transferred from the EU was not maintained. Regarding international agreements concluded between the UK and non-EU/EEA countries, the

European Commission should examine the interplay between the UK data protection framework and its international commitments.

[EDPB Opinion 32/2021 on the assessment of the adequate protection of personal data in the Republic of Korea](#). The EDPB invited the European Commission to clarify issues pertaining to the right to withdraw consent; information given to individuals about onward data transfers; the concept of pseudonymisation; and access by public authorities to personal data transferred to the Republic of Korea.

## **EDPB work on dispute resolution and urgency procedures**

In 2021, we also provided substantive contributions to the drafting of the guidelines and decisions in relation to Article 65 enables the EDPB to adopt binding decisions in cases where national DPAs cannot agree on some elements of interpretation of the GDPR. Article 66 allows any DPA, under certain conditions, to request an urgent opinion or an urgent binding decision from the EDPB where a competent DPA has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of individuals.

Some examples are listed below.

[EDPB Guidelines 03/2021](#) on the application of Article 65(1) (a) GDPR. Article 65(1) (a) of the GDPR is a dispute resolution mechanism meant to ensure the correct and consistent application of the GDPR in cases involving cross-border processing of personal data. It aims to resolve conflicting views amongst the Lead Data Protection Authority (DPA) and Concerned Data Protection Authority on factors in a case. These Guidelines explain the application of Article 65(1) (a) GDPR. Specifically, these Guidelines explain the application of the relevant provisions of the GDPR and the EDPB's Rules of Procedure, outline the main stages of the procedure and explain the competence of the EDPB when adopting a legally binding decision on the basis of Article 65(1)(a) GDPR.

[EDPB Article 65 GDPR decision on WhatsApp Ireland](#). This binding decision addressed the dispute that arose following a draft decision issued by the Irish DPA as Lead DPA regarding WhatsApp Ireland Ltd. Following its assessment, the EDPB stated that the Irish DPA should amend its draft decision regarding infringements of transparency, the calculation of the fine and the period for the order to comply.

In 2020, the EDPS [proposed](#) the establishment of a Support Pool of Experts (SPE) within the EDPB, with the aim to assist DPAs in dealing with complex and resource intensive cases.

The EDPS also assisted the EDPB in other ways, for example in regard to the EDPB's:

- cooperation with the European Commission in the context of the latter's initial and in-depth [investigation](#) during 2020 of the proposed Google-Fitbit merger;
- [Statement](#) and [FAQ](#) during July 2020 to provide the first answers on the impact of the "[Schrems II](#)" ruling; and
- [Guidelines 9/2020 on relevant and reasoned objection](#).



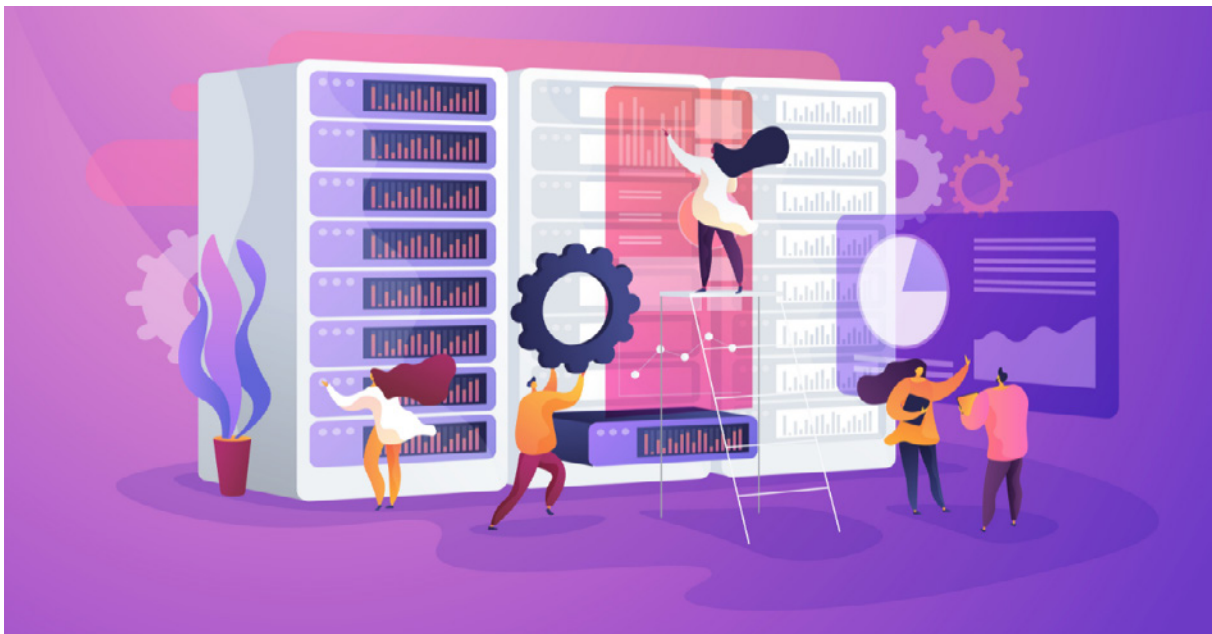
## Building strategic partnerships to strengthen data protection

The EDPS continued to foster, maintain and deepen collaboration with other privacy and data protection outside the EU, as well as EU institutions of strategic importance to ensure the coherent protection of individuals' privacy and personal data.

For example, during COVID-19, the EDPS deemed it necessary to strengthen its cooperation with the EU Agency for Fundamental Rights, especially in the context of the use of contact-tracing apps and its possible interference with fundamental rights if miss-used or abused. Reflecting the same goals to protect people and their freedoms during the health crisis, [a memorandum of understanding was updated on 20 June 2022](#).

Recognising the importance of pairing up cybersecurity efforts with data protection to protect individuals and their rights, the EDPS also [signed a memorandum of understanding with ENISA](#), the European Union Agency for Cybersecurity in November 2022. This strategic cooperation allowed us design, develop and deliver capacity-building, awareness-raising activities, as well as cooperating on policy-related matters on topics of common interest, and contribute to similar activities organised by other EU institutions.

Building our research and foresight capacity of technologies, the EDPS has also partnered with the Spanish Data Protection Authority by [signing a Memorandum of Understanding on 29 June 2023](#). Together, we have worked on a series of joint initiatives for raising awareness on future technological trends.



Beyond the EU, the international dimension of data protection has been of great importance, especially with the UK's Information Commissioner's Office (ICO) with whom the EDPS shares experiences and best practices; cooperates on specific projects of interest; share information or intelligence to support their regulatory work; and promote dialogue amongst data protection authorities and other digital regulators. To this effect, [a memorandum of understanding](#) was signed with ICO on 9 November 2023.



## International Fora and platforms

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

### Global Privacy Assembly

The EDPS continued to contribute to the activities of the [Global Privacy Assembly \(GPA\)](#), an international forum that brings together more than 130 data protection and privacy authorities from across the globe.

The EDPS is co-chair of the GPA working group on Ethics and Data Protection in AI (AIWG). The EDPS also takes part to other GPA working groups (Global Frameworks and Standards, Digital Economy, Data Protection and Other Rights Freedoms, International Enforcement Cooperation, Digital Citizen and Consumer, The Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management, Data Sharing, etc).

Over its mandate, the EDPS has sponsored or co-sponsored on a number of GPA resolutions and partook in a variety of its working groups.

This includes, in particular, sponsoring the [GPA Resolution on Generative AI Systems](#), which endorses the existing data protection and privacy principles as core elements for the development, operation, and deployment of generative AI systems and provides initial guidance on how these principles apply in this specific context. Another recent example is the GPA Resolution on Data Free Flow with Trust (DFFT). This resolution presented by the EDPS and the Federal German DPA advocates for and promotes the initiatives developed under the concept of DFFT as a banner to promote high standards for data protection and privacy for an efficient regulation of global data flows, identifies high-level elements the GPA regards as essential to achieve secure and trustworthy cross-border data flows and makes a number of proposals to operationalise the concept of DFFT.

Other Resolutions that the EDPS co-sponsored include the Resolution on principles regarding the processing of personal information in neuroscience and neurotechnology, the Resolution on Health Data and Scientific Research, the Resolution on Achieving global data protection standards, the Resolution on AI and Employment, the Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology or the Resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes .

### International Organisations Workshop

Pursuing our aim to foster global partnerships in the field of data protection, the EDPS continues to co-organise with a different International Organisation its workshops to share experiences and best practices in the field of privacy and data protection. Participants discuss the most recent regulatory developments at international level and analyse their implications for International Organisations.

During this mandate, the EDPS co-hosted workshops:

- In 2020, online, covering the topics on the impact of the global pandemic on data protection, COVID-19 certifications, and security of teleworking.
- In 2022, with the World Food Programme on the impact of the global pandemic on data protection and the humanitarian field; individuals' rights; data breach response; international data transfers; privacy risk management and disinformation.
- In 2023, with INTERPOL, on trends in privacy and data protection; data transfers to and between International Organisations.
- In 2024, with the World Bank, the development and use of artificial intelligence in International Organisations; personal data breaches; compliance of IT tools.

Continuing these International Organisations Workshops, since their creation in 2005, is crucial as they are a driving force behind global progress in data protection.

## **Roundtable of G7 data protection and privacy authorities**

Since 2022, the EDPS participated in the annual [G7 Data Protection and Authorities Roundtable](#), representing the EU alongside the EDPB, and bringing together data privacy regulators from the G7 countries, i.e. Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

Collaborating with our partners from like-minded G7 countries is one way of creating common approaches to privacy and data protection in this fast-moving landscape. It is a valuable opportunity to promote EU data protection standards on the world stage and build deeper cooperation based on shared values.

Over the years, the EDPS has collaborated on topics such as data free flow with trust; emerging technologies; and enforcement cooperation; the intersection of privacy, competition and consumer protection; AI and Children.

## **EDPS-Western Balkans and Eastern Partnership Region**

In the last two years of its mandate, the EDPS has taken part in high-level events titled "Data Protection in the Western Balkans and Eastern Partnership Region", to discuss and exchange with representatives from data protection authorities and public institutions from Albania; Armenia; Azerbaijan; Bosnia and Herzegovina; Georgia; Kosovo; Moldova; Montenegro; North-Macedonia; Serbia and Ukraine.

These meetings have proved fruitful to discuss the challenges, opportunities, and approaches on compliance and enforcement of data protection as supervisory authorities.

In particular, discussions were centred on exchanges on policy aspects, on technology monitoring, on supervision and enforcement methodologies, on transfers, on AI regulation as well as on the new European data regulations.

This partnership confirms that international cooperation in data protection is not an option, but vital to our tasks.

## Council of Europe

[The Council of Europe](#) is an important player in privacy and data protection law and policy, not only in Europe but increasingly on other continents where pan European norms are often taken as a source of inspiration for legislation and policies.

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ([Convention 108](#)) is open to accession by both European and non-European countries. The Convention 108 has been recently [modernised](#) to deal with challenges resulting from the use of new information and communication technologies and to strengthen the Convention's effective implementation. In mid-January 2024, 31 States have ratified the Amending Protocol and seven ratifications are still required for the entry into force of the modernised Convention 108.

The EDPS is an observer at the Council of Europe's expert groups on data protection, including the Consultative Committee (T-PD) of Convention 108 and represents the Global Privacy Assembly before the T-PD.

The EDPS also follows the ongoing negotiations on a Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, in the framework of the Committee on Artificial Intelligence (CAI).

We attend the meetings of these expert groups and provide informal oral and written comments with a view to ensure a good level of protection and compatibility with EU data protection standards.

## Spring Conference

The data protection authorities from the Member States of the EU and of the Council of Europe meet annually for a European Conference, also called the "Spring Conference" to discuss matters of common interest and to exchange information and experiences on different topics. The EDPS actively contributes to the discussions. The conference usually ends with the adoption of a number of resolutions, available on the EDPS website.

The EDPS regularly participates in the annual case-handling workshops organised by national data protection authorities (DPAs) and supervisory authorities in Europe (including non-EU countries).



These workshops are useful fora to discuss practical issues at working level and bring together DPAs staff (complaint handlers and inspectors in particular) from all over Europe.

[More information on EDPS' involvement in the Spring conference.](#)

## **OECD**

The EDPS participates as an observer to different working parties of the OECD, in particular the Working Party on Data Governance and Privacy (DGP), which is attached to the Committee on Digital Economy Policy, and the Working Party on Artificial Intelligence (AIGO).

The OECD and the EU share common values as regards the need for the digital transformation to be human-centric and fundamental rights-oriented.

We provide, when necessary, comments to the Working Party on recommendations relating to the protection of privacy and data protection.

## **Berlin Group**

The International Working Group on Data Protection in Telecommunications ([IWGDPT](#)), also known as the Berlin Group, aims to contribute to ensuring at international level a consistent and high level of data protection and privacy, based on democratic principles and fundamental rights, by identifying emerging technologies and delivering positions and practical advice on them.

The Chair of the Group is the German Federal Commissioner for Data Protection and Freedom of Information (BfDI). The Group is composed of representatives of worldwide data protection supervisory authority as well as of some independent experts representing various sectors, including public authorities, private organizations, academia and civil society.

The EDPS regularly participates in the meetings and contributes to the various activities of the Group, in particular by leading or supporting the drafting of their papers.

## **EDPS Opens Strasbourg Office**

On 14 March, the EDPS has opened his new Office in the premises of the European Parliament in Strasbourg.

With the new 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. Data protection is becoming increasingly engrained in EU legislation, the new EDPS office provides an opportunity for closer cooperation and engagement with policymakers and other EU institutions present in Strasbourg, as well as with the Council of Europe.

The inauguration ceremony featured speeches from the Chair of the LIBE Committee of the European Parliament, the European Ombudsman and the Council of Europe.

## EDPS Conferences

Alongside participating to conferences, the EDPS has also provoked debates, and built a long-term vision for the future of data protection.

### The future of data protection: effective enforcement in the digital world

In June 2022, we organised and hosted a [hybrid conference of 2000 participants, titled “The future of data protection: effective enforcement in the digital world”](#), focusing on the need for effective enforcement, and collective consideration for building a culture compliance, as well as on the GDPR’s governance model and its areas for improvement. Supervisor Wojciech Wiewiórowski stated that he strongly believes that a pan-European data protection enforcement model is going to be a necessary step to ensuring real and consistent high-level protection of the fundamental rights to data protection and privacy across the European Union (EU).

Topics during the conference included:

- Judicial remedies and enforcement of data protection
- Enforcement in the public sector
- How foresight can support data protection?
- Efficient enforcement through innovation

### European Data Protection Summit: rethinking data in a democratic society

In July 2024, the EDPS took the opportunity of its [20th Anniversary to organise a Summit to rethink data in a democratic society](#).





## EUROPEAN DATA PROTECTION SUMMIT

It is the moment to collectively discuss what must be done to tackle the ever-growing accumulation of information on individuals, by private or public entities, and what privacy and data protection should do to advance and safeguard our democracies.

**Wojciech Wiewiórowski**  
The European Data Protection Supervisor



Bringing together global actors in privacy and technology, we aimed to bring at the forefront of the public debate questions about the role of a state in times of ever-growing collection of information about citizens, be it by private or public entities, and the part that data protection should play in modern democracies.

Discussion will touch upon the role of data protection, its possibilities and limitations, its successes and missed opportunities, in contributing to the development of the fundamentals of democratic societies. Through this initiative, the EDPS seeks to foster and fuel the public debate on this matter by rethinking present and future needs.

Topics covered included:

- Gatekeepers of dis/information and the role of institutions in protecting democracy
- Is data protection law suitable for public authorities?
- How to build a functioning democratic oversight?



## CHAPTER NINE

# ***Leading with independence and integrity***



One of the EDPS' core values is to lead with integrity and impartiality, to uphold the highest standards of behaviour and to always do what is right, being independent and objective.

To achieve this, the EDPS has put in place a system of checks and balances to hold itself accountable through the work of the Data Protection Officer, the Transparency Officer, the Internal Control Coordinator, together with functions covering planning coordination and records, archives and knowledge management—in the Governance and Internal Compliance Unit.

Under the lead of the Internal Control Coordinator, the unit coordinated the preparation of the Annual Activity Report and the risk management exercise, acted as contact point for the European Court of Auditors and the Internal Audit Service, monitored and reported on business processes and quality management, thus contributing to compliance and preparedness activities for the organisation.

Furthermore, the unit coordinated the internal planning and the preparations for the annual management plan that translates the strategy of the EDPS for the mandate into general and specific objectives.

Between 2023 and 2024 the G&IC unit steered the on-boarding and implementation of the ARES (Advanced Records System) application for administrative activities and continued to ensure the maintenance of the EDPS Case Management System (CMS) for core business activities, whilst continuing to advise and support staff on records and knowledge management related matters.

As an EU institution, and according to Regulation (EU) 2018/1725 and our Rules of Procedure, the EDPS is subject to Regulation (EC) 1049/2001 on public access to documents. The Transparency Officer coordinated the application of the regulation within the EDPS, observing a steadily growing number of requests during the mandate.

Following up on the European Parliament's recommendations in the context of the EDPS' discharge procedures, and in line with its continued commitment to transparency, the EDPS started examining the available options for joining the inter-institutional agreement on a mandatory transparency Register in 2023. Based on the assessment of applicable rules and procedures, and taking into account the EDPS context, it was decided to take the necessary steps to adopt conditionality and/or complementary transparency measures, and request the publication of such measures on the Transparency Register webpage.

## **The EDPS' data protection officer**

The EDPS' data protection officer is an independent function, and its establishment is required by Regulation (EU) 2018/1725.

The focus of the DPO at the EDPS during this mandate was to continue the process of a smooth transition towards the data protection framework set out in Regulation (EU) 2018/1725, while always keeping the role and mission of the EDPS in mind.

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, we therefore continued to strengthen our accountability by raising the standard of compliance of the ongoing and new personal data processing activities, including seeking privacy and data protection friendly alternatives.

Considering the EDPS' role as the data protection authority (DPA) of the 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 raise and uphold the highest standards of data protection. 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 DPO focused on putting accountability into practice, for example, by updating data protection notices and making them available to the public in multiple languages, as well as updating the register for processing activities.

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.

Likewise, the DPO advised and worked closely with the services of the EDPS in charge of processing personal data in order to ensure the institution's compliance with data protection law and principles. This has included providing advice to the EDPS' human resources, information security and communications services so that they can put in place the appropriate safeguards or set up the contractual terms tailored

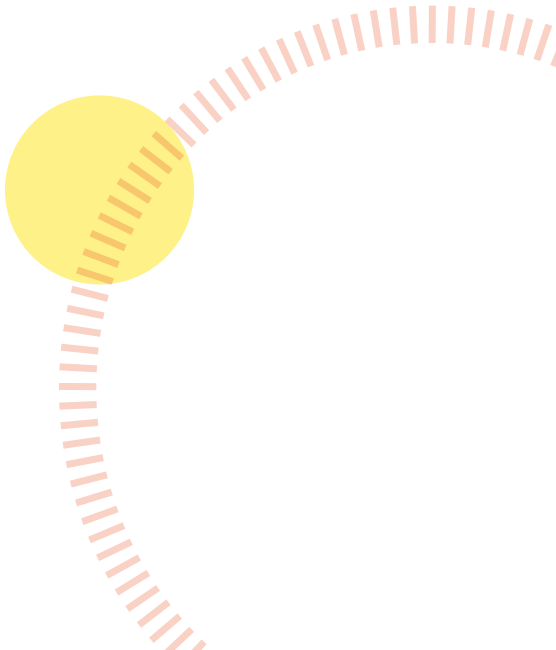


to the relevant circumstances. The DPO was also regularly consulted on the legal provisions of new and updated agreements with EUIs as service providers for the EDPS; new and updated contracts with external service providers; and the review of certain internal rules and procedures.

As part of its role, and like any other DPO of an EU institution, the EDPS' DPO has addressed a number of enquiries, complaints and requests from individuals. These include erasure requests, access requests, information requests, and rectification requests from individuals concerning their personal data.

Adjacent to this, the EDPS pursued activities to raise awareness about data protection through training sessions and other outreach activities.

Additionally the DPO continued its collaboration with the other data protection officers of the EU institutions and data protection authorities of the EU/EEA.



## CHAPTER TEN

# *Being recognised and recognisable as the EU institutions' data protection authority*



Public interest in and engagement with data protection and the work of data protection authorities (DPAs) has grown steadily over the mandate, more so in light of the increasing digitalisation of individuals' daily lives. People are more aware of and concerned about their digital footprint and the importance of protecting their personal data. The EDPS Information and Communication team aimed to therefore ensure that EDPS activities and messages reach the relevant audiences at the right time.

The role of the team, reinforced in the EDPS Strategy 2020-2024, was to explain and promote the work of the EDPS. This committed us to making data protection issues, in particular the impact that processing operations and technologies might have on individuals and their personal data, more accessible to a large audience by providing information on the EDPS's day-to-day work in clear language and via appropriate communication tools.

Our main channels of communication during this mandate has been the EDPS website, social media platforms, X, LinkedIn, EU Voice, EU Video, as well as through the organisations of events.

### **Websites**

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.

Over the mandate, the EDPS has also created dedicated websites to draw our audience's attention to our different priorities. This includes:

- a dedicated website to present the [EDPS Strategy 2020-2024](#) with our priorities for the mandate in an interactive way to make it more appealing and accessible to a wider audience so that they can easily navigate our three strategic pillars;
- a dedicated website for [CPDP Data Protection Day Conference](#)
- a website for our EDPS Conference: "[The future of data protection: effective enforcement in the digital world](#)"
- a website for the [EDPS' 20th anniversary](#).

## 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 6000 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.

## A new visual identity for a new mandate

In 2020, we developed a new visual identity for the EDPS, which will be used for our promotional items, publications and website. Based on this, we also developed an [EDPS corporate brochure](#) and [video](#), which will be shared with the public in 2021.

Our new visual identity reinforces our corporate identity and reflects the role of the EDPS as a global leader in data protection and privacy not only in the EU, but also beyond. It also marks a new era in the history of the EDPS, which will focus more on shaping a safer digital future.

## Social Media

In this highly digitised world, social media has become one of the most common communication tools. Over the years, we have built a well-established presence on three social media channels, namely X (formerly known as Twitter), LinkedIn and YouTube, which we use to reach a global audience easily and quickly. In 2024, we also opened an EDPS account on [Instagram](#) to better interact with a younger audience through engaging communication reels and images.

Our [@EU\\_EDPS X account](#) allows us to promote the EDPS' presence at a variety of events and to feature the core messages and purpose of our work.

We use our [European Data Protection Supervisor LinkedIn account](#) to communicate with a more specialised audience and other actors interested in the field of privacy and data protection. LinkedIn remains our fastest-growing channel with the highest number of actively engaged followers.

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



As part of our goal to seek alternative communication tools that promote a more democratic, decentralised and privacy-friendly model of social media, we multiplied our presence on our social media platforms: EU Voice and EU Video based on free and open source [Mastodon](#) and [Peertube](#) software, launched in February 2022 to serve as additional communication channels to our X and LinkedIn accounts.

Using our various social media channels, we planned and executed a variety new and recurrent social media campaigns, to increase our outreach and keep our audience informed about our activities.

**#InCaseYouMissedIt:** As we continue to welcome new followers to our ever-growing social

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

**European Cybersecurity Month:** Each year we have created factsheets, including a comic and a podcast episode to raise awareness on different aspects of cyber hygiene.

## Our podcast channel: EDPS On Air

In December 2022, we started a new podcast series, with the aim of bringing our audience closer to the work we do to shape a safer digital future, in just under 10 minutes.

Each episode includes selection of updates on our latest work in the fields of Supervision & Enforcement, Policy & Consultation, Technology & Privacy. This podcast series complements the EDPS' monthly newsletter by sharing our latest activities on a different platform; we aim to cater for our different audience groups.

Now active for two years, and with more than 15 episodes published, the Newsletter Digest Podcast has evolved, with bonus episodes including exclusive interviews with actors in the data protection field.

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

All podcasts produced by the EDPS are accessible on our [EDPS On Air channel on our website](#). It is also possible to subscribe to our podcast series via our Podcast RSS Feed. In 2023, we also opened a space on [Spotify](#) to increase the accessibility of our podcast content and grow our audience on a specialised platform. There, we strive to create a variety of informative and entertaining content to suit all interests in data protection. From interviews with thought-provoking experts, to deep dives into current events, our goal is to provide information on EDPS' work and to explore the EU data protection and privacy framework.

## **20 Talks: a series of insightful discussions**

To mark the EDPS' 20th anniversary, the Information and Communication Unit produced [a series of talks](#) with 20 experts and influential personalities across diverse domains, looking into profound implications of privacy and data protection within their specific spheres.

## **An increase in events, a rising interest in our work**

The appetite of our community to engage in pivotal and current data protection issues continues to grow. The I&C Unit supports the EDPS in its mission to interact with various actors, including data protection and technology experts, EU and national legislators, to help advance the global standards of data protection. This includes the organisation of workshops and seminars, Europe Day, Study visits, Data Protection Day.

## **Public Relations**

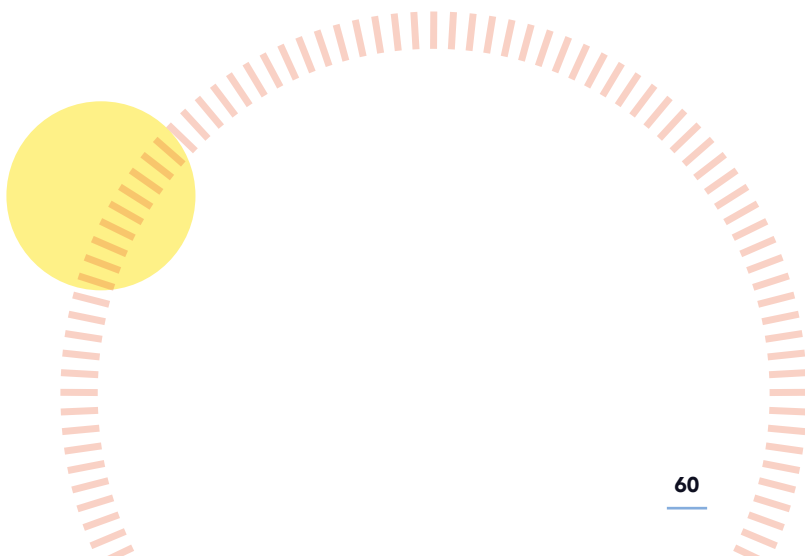
Throughout the mandate, we frequently interacted with the media through press releases, interviews and press events on topics such as the GDPR, transfers of personal data, combatting sexual abuse, data breaches, artificial intelligence to name a few examples.

## **The EDPS' employer branding strategy**

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 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 also delivered 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.



## CHAPTER ELEVEN

# ***Reshaping our organisation to meet data protection challenges***



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

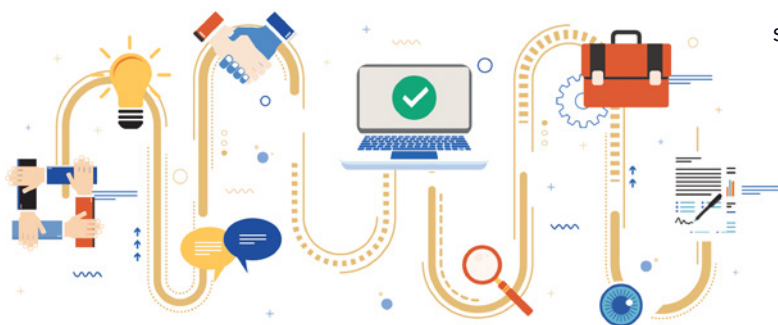
HRBA accompanied [the organisation's expansion and growth over the mandate](#). This included the establishment of the EDPS' Strasbourg office in March 2023. The office was established to support the EDPS Strategy's objective to reinforce its inter-institutional and international cooperation. By setting 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.

The EDPS saw other significant organisational changes throughout the mandate.

- In the Supervision and Enforcement unit, the creation of three specific sectors: one to monitor and ensure compliance in the EU's Area of Freedom, Security and Justice (ASFJ sector); a sector to address efficiently complaints made by individuals and to launch timely investigations into the way personal data is processed (Complaints and Investigations sector), and a sector to deliver comprehensive advice to EUIs on data protection matters and through data protection audits (Consultation and Audits sector).
- The restructuring of the former IT policy sector into a fully-fledged EDPS' Technology and Privacy Unit to ensure that technologies embed the principles of privacy and data protection. This includes the creation of a specialised sector to ensure thorough oversight and auditing of IT systems; a

sector to anticipate new technologies and their impact on privacy and data protection; and a sector to develop the independent digital transformation of the institution.

- A dedicated Legal Service in 2021 for specialised assistance on the EDPS' case files.
- The appointment of the EDPS Secretariat-General in 2023, to coordinate the EDPS' actions to ensure the effective functioning of the EDPS; support the Supervisor in engaging with the EDPS' stakeholders and other actors in the fields of data protection and privacy in the EU and beyond.
- The Governance and Internal Compliance Sector created in 2022 and upgraded into a unit in 2023 with the aim to create synergies between internal compliance and data protection obligations, transparency and access to documents, internal control coordination, records, archives and knowledge management for example, to enhance the EDPS' accountability and to support its compliance with applicable laws and obligations.
- The creation of an AI Unit in October 2024 to prepare for our role as AI Supervisor, market surveillance authority and notified body for the EU institutions.



Investing in the wellbeing and sustainability of its staff and workforce, the EDPS has adapted its working conditions, improved the work environment by refurbishing the premises and overhauling “kitchenettes” and public spaces on each floor, organised an artistic Data-protection related exhibition, focused on the professional development of its staff, retaining colleagues, but also seeking diverse and specialised talent to shape the

world of data protection and our organisation.

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

## **Overcoming challenges during the COVID-19 pandemic**

Following the European Parliament's approach, we decided in March 2020 to prohibit access to the EDPS building to those returning from regions that had a significant risk of COVID-19 infection for fourteen days after the journey. In the same vein, the EDPS cancelled events, seminars and meetings in the EDPS building with immediate effect.

The Extended Management Board of the EDPS, acting as Business Continuity Team, approved the contingency plan with the aim to prepare for a possible pandemic. This included a test to assess whether the EDPS was ready to switch to remote working in terms of technical requirements and capacities.



Following the World Health Organisation's (WHO) declaration of COVID-19 as a pandemic and the subsequent request to governments and organisations to appropriately react to the pandemic threat, the EDPS entered the phase of work modality 0 (100% teleworking without access to the EDPS building).

HRBA closely followed the evolution of the pandemic and aligned its administrative decisions with the measures put in place by the Belgian authorities as well as measures adopted by other EUIs.

During the following months and during work modality 0, HRBA, instructed by the Director, limited access to the EDPS building to those who needed to carry out essential tasks which could not be accomplished remotely, regularly sent communications encouraging EDPS staff to continue to follow hygiene and safety instructions. HRBA also made signs to guide EDPS staff around the building to maintain social distancing, as well as other signs to remind them to wear masks and to use disinfectant available in the building to ensure safe working conditions.

In June 2020, the EDPS, harmonising their approach with the Belgian authorities and other EUIs, went into work modality 1. Teleworking was still the norm, but EDPS staff could voluntarily return to the building, in particular those who had difficulties performing their tasks from home. The maximum occupancy rate per floor was fixed at 30%. The EDPS also adopted the decision on additional measures to limit the spread of COVID-19.

Given the significant rising infection rate in October 2020, the Belgian government declared telework compulsory by law. Thus, the EDPS stayed in work modality 1 while reducing the presence rate to 15% up until the end of January 2021 and asked colleagues to keep teleworking unless their visit to the premises was strictly necessary for essential tasks and was authorised by the line manager.

## **Budget**

In the past, the EDPS experienced challenges with its budget implementation, in particular as a consequence of the COVID-19 pandemic. However, the KPI related to budget implementation has been exceeded during the last years. Adaptations had to be made in the work programme to reflect budget restrictions as a consequence of the reduced budget allocations by the budgetary authorities, growing responsibilities of our organisation and to reflect the EU's unprecedented inflation rate.

To monitor, forecast and boost our efficiency in this area, we implemented the Bluebell Budget Software in 2023.

Bluebell also allows us to give a refined view of all budget lines by detailing them into actions and linking these actions with posting criteria in ABAC, the financial software used in the European Commission and other EUIs, so that the forecast can be compared in real time with the actual execution. Using this system has increased our efficiency in the preparation, monitoring and follow-up of budget execution. In addition, the tool proves to be useful for audit trail purposes and ex-post control as files and supporting documents are available anytime in the system.

## CHAPTER TWELVE

# Celebrating the EDPS 20<sup>th</sup> Anniversary



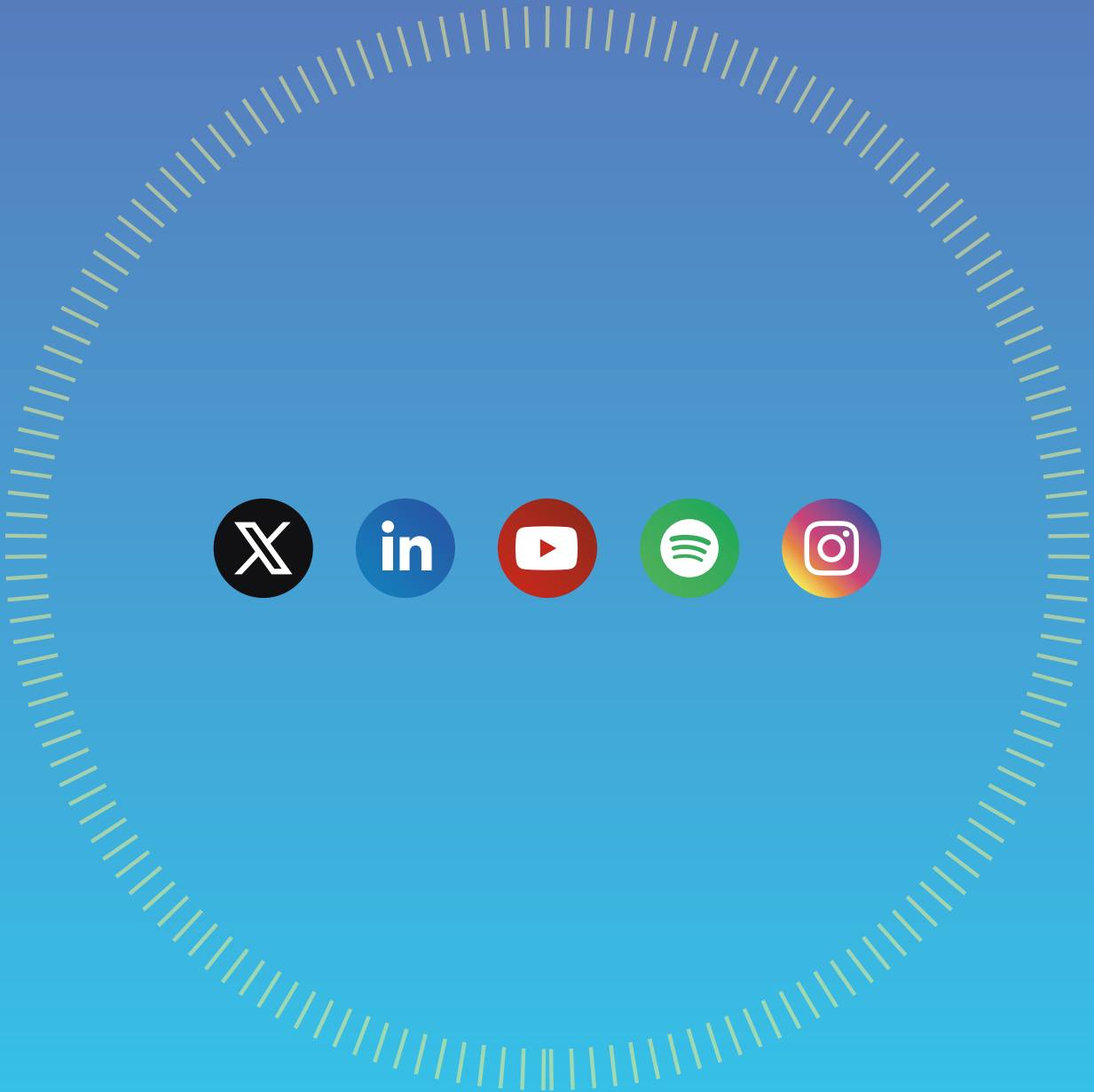
2024 marked the EDPS' 20th anniversary of being the EU's independent institution in charge of supervising the way EU institutions process individuals' personal data.

The EDPS' 20th anniversary as an opportunity to take stock of the past and to build on the present to approach the upcoming challenges in a way that respects individuals' privacy and leaves no one behind.

On this occasion, we worked on four pillar activities:

- A **[book](#) (20 years of data protection. What next?)** and a **[timeline](#)** that analyses key data protection milestones and the EDPS' influence and history in this remit over the last two decades, as well as an in-depth analysis of what is yet to come.
- To inform our work as a data protection authority going forward, we must also be able to learn from others. **Our second pillar comprises [20 talks with leading voices from around the world](#)** who share their unique perspective on how data protection and privacy shapes their respective fields.
- With a view of modernising the EDPS' approach to anticipate and tackle future challenges, **our third pillar includes [20 initiatives](#) aimed at further emboldening individuals' fundamental rights.**
- The **fourth pillar is our [European Data Protection Summit–Rethinking Data in a Democratic Society](#)**, which took place on 20 June 2024, in Brussels, Belgium. During this event, we encouraged dynamic and open discussions on the role of privacy and data protection in modern democracies by examining, in particular, the role of a state at a time of an ever-growing collection of information about citizens.





Publications Office  
of the European Union

