



EUROPEAN DATA  
PROTECTION SUPERVISOR

# ANNUAL REPORT 2021

An executive summary of the Annual Report 2021, which gives an overview of the key developments in EDPS activities in 2021, is also available.

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.

Waterford, Ireland – Brussels, Belgium: Trilateral Research Ltd, Vrije Universiteit Brussel, 2022

© Design and Photos: Trilateral Research Ltd, EDPS & European Union

© European Union, 2022

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.

PDF ISBN 978-92-9242-708-5 ISSN 1830-9585 doi: 10.2804/90062 QT-AA-22-001-EN-N

HTML ISBN 978-92-9242-707-8 ISSN 1830-9585 doi: 10.2804/146741 QT-AA-22-001-EN-Q

# TABLE OF CONTENTS

<b>FOREWORD</b>	<b>12</b>
<b>MISSION, VALUES AND PRINCIPLES</b>	<b>15</b>
<b>EDPS STRATEGY 2020-2024</b>	<b>18</b>
<b>CHAPTER ONE: AN INTRODUCTION TO THE EDPS</b>	<b>20</b>
1.1.About the EDPS	21
1.2.Supervision and Enforcement	22
1.3.Policy and Consultation	24
1.4.Technology and Privacy	25
<b>CHAPTER TWO: 2021 HIGHLIGHTS</b>	<b>27</b>
2.1.International transfers of personal data	28
2.2.COVID-19 and data protection, our efforts continue	29
2.3.Supervising the Area of Freedom, Security and Justice	30
2.4.Shaping Europe's Digital Future	32
2.5.An increase in legislative consultations	34
2.6.Pleadings before the Court of Justice of the European Union	35
2.7.A new initiative, TechSonar	37
2.8.Human Resources, Budget and Administration	38
2.9.The EDPS' Communication Activities	39
2.10.Key Performance Indicators	40
<b>CHAPTER THREE: SUPERVISION AND ENFORCEMENT</b>	<b>42</b>
3.1.Transfers of personal data to non-EU/EEA countries	43
3.2.COVID-19 and data protection, our efforts continue	49

3.3. EDPS Cooperation with EUIs' data protection officers	52
3.4. Addressing complaints from individuals	57
3.5. Data Protection audits	62
3.6. EDPS investigations	66
3.7. The EDPS' advisory powers	68
3.8. Cooperation with the EFTA Surveillance Authority	78

## **CHAPTER FOUR: THE SUPERVISION OF THE AREA OF FREEDOM, SECURITY AND JUSTICE 80**

4.1. A holistic approach to the supervision of AFSJ bodies and agencies	81
4.2. Supervising Europol	83
4.3. Supervising EPPO	93
4.4. Supervising Eurojust	94
4.5. Supervising Frontex	95
4.6. Supervision of large-scale IT systems	96

## **CHAPTER FIVE: TECHNOLOGY AND PRIVACY 100**

5.1. TechDispatch receives an award	101
5.2. Our new initiative: TechSonar	102
5.3. Personal data breaches	103
5.4. Cooperation with data protection authorities in technology and privacy matters	114
5.5. Cybersecurity training session for EDPS colleagues	116
5.6. IPEN workshops	117
5.7. Digital sovereignty and digital transformation	118



5.8. Website Evidence Collector 1.0	120
5.9. Eurodac Inspection Report	121
<b>CHAPTER SIX: LEGISLATIVE CONSULTATIONS</b>	<b>122</b>
6.1. An increase in Informal and Formal Legislative Consultations	124
6.2. Key Opinions issued in 2021	125
6.3. EDPS-EDPB Joint Opinions	131
6.4. Key formal comments issued in 2021	134
6.5. Case Law Digest on Transfers of Personal Data	137
<b>CHAPTER SEVEN: THE EDPS AS A MEMBER OF THE EDPB</b>	<b>139</b>
7.1. Enforcement, support and coordination	140
<b>CHAPTER EIGHT: INTERNATIONAL COOPERATION</b>	<b>147</b>
8.1. The 43rd Global Privacy Assembly	148
8.2. Council of Europe	149
8.3. The Computers, Privacy and Data Protection Conference	150
8.4. Cooperation with International organisations	152
<b>CHAPTER NINE: COOPERATION WITH CIVIL SOCIETY</b>	<b>153</b>
<b>CHAPTER TEN: TRANSPARENCY AND ACCESS TO DOCUMENTS</b>	<b>156</b>
<b>CHAPTER ELEVEN: THE EDPS' COMMUNICATION ACTIVITIES</b>	<b>158</b>
11.1. The EDPS' corporate image	159
11.2. Our social media channels	160

11.3.EDPS Website	162
11.4.Publications	163
11.5.Virtual and in-person events	165
11.6.External relations	168
11.7.Employer branding	170
11.8.Preparing the EDPS Conference	171

## **CHAPTER TWELVE: HUMAN RESOURCES,BUDGET**

### **AND ADMINISTRATION 173**

12.1.A safe return to the office	174
12.2.Well-being at work	175
12.3.Recruiting data protection experts	177
12.4.Employer branding	177
12.5.Adapting our working conditions	178
12.6.Budget	180
12.7.Public Procurement	182
12.8.Learning and development	183
12.9.The European House of Data Protection	184

## **CHAPTER THIRTEEN: THE EDPS' DATA PROTECTION OFFICER 185**

13.1.Accountability	186
13.2.Advising the EDPS	189
13.3.Enquires and complaints	190
13.4.Raising awareness about data protection	193
13.5.Cooperation	193

<b>ANNEX A - LEGAL FRAMEWORK</b>	<b>195</b>
<b>ANNEX B - EXTRACT FROM REGULATION (EU) 2018/1725</b>	<b>201</b>
<b>ANNEX C - LIST OF DATA PROTECTION OFFICERS</b>	<b>208</b>
<b>ANNEX D - LIST OF EDPS OPINIONS</b>	<b>216</b>
<b>ANNEX E - LIST OF EDPS FORMAL COMMENTS</b>	<b>218</b>
<b>ANNEX F - LIST OF EDPS-EDPB JOINT OPINIONS</b>	<b>226</b>
<b>ANNEX G - EDPS WORK WITHIN THE EDPB</b>	<b>228</b>
<b>ANNEX H - THE SUPERVISOR'S SPEECHES</b>	<b>232</b>
<b>GETTING IN TOUCH WITH THE EU</b>	<b>236</b>

## TABLES AND GRAPHS

Figure 1: Key Performance Indicators	41
Figure 2: Statistics of complaints received	62
Figure 3: Europol Statistics 2021	92
Figure 4: Number of Personal Data Breach Notifications per month in the year 2021	106
Figure 5: Number of Personal Data Breach Notifications per month for the years 2019-2021	106
Figure 6: Root Cause of the Personal Data Breaches	108
Figure 7: Comparison Chart on the Root Cause of the Personal Data Breaches 2019-2021	108
Figure 8: Type of Personal Data Breaches	109
Figure 9: Type of Data Breach Notification	110
Figure 10: Impact of Personal Data Breaches	111
Figure 11: Special Categories of data in personal data breaches notifications	112
Figure 12: Notification to the Data Subject	113
Figure 13: Evolution of legislative consultations since 2018	125
Figure 14: Statistics on Communication Activities	172
Figure 15: Type of requests processed by the DPO of the EDPS in 2021	191
Figure 16: Evolution of data subject requests since 2019	192
Figure 17: Evolution of complaints since 2019	192

The background is a dark blue gradient with a complex network of thin, light blue lines connecting various sized dots, creating a web-like or molecular structure.

# **ABBREVIATIONS**


AFSJ	Area of Freedom, Security and Justice
AI	Artificial Intelligence
CMS	Case Management System
CPDP	Computers, Privacy and Data Protection Conference
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EURODAC	European Asylum Dactyloscopy Database
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EES	Entry/Exit System
ESA	European Free Trade Area (EFTA) Surveillance Authority
EPPO	European Public Prosecutor's Office
ETIAS	European Travel Information and Authorisation System
EU	European Union
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the AFSJ
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EUIs	European Union institutions bodies, offices and agencies
Frontex	European Border and Coast Guard Agency

GDPR	Regulation (EU) 2016/679, General Data Protection Regulation
GPA	Global Privacy Assembly
HR	Human Resources
HRBA	Human Resources, Budget and Administration Unit
ICT or IT	Information and communications technology
ICDPPC	International Conference of Data Protection and Privacy Commissioners
IPEN	Internet Privacy Engineering Network
LED	Directive 2016/680, Law Enforcement Directive
MoU	Memorandum of Understanding
P&C	Policy and Consultation Unit
PET	Privacy Enhancing Technology
S&E	Supervision and Enforcement Unit
SIS II	Schengen Information System
SLA	Service Level Agreement
SCCs	Standard Contractual Clauses
SCG	Supervision Coordination Group
SPE	Support Pool of Experts
T&P	Technology and Privacy Unit
TIA	Transfer Impact Assessment
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
VIS	Visa Information System

The background is a dark blue gradient with a complex network of thin, light blue lines connecting various sized dots, creating a web-like or molecular structure. The dots and lines are more concentrated on the left side and become sparser towards the right.

# **FOREWORD**





During my [closing remarks](#) at the Computers, Data Protection and Privacy conference in January 2021, I shared with participants my feelings of hope. Hope that we will come out of the solitude of lockdowns with a shared, common experience of having gone through this for each other; that the solidarity we had been experiencing will make us stronger as a society; and that this shared experience is something that we will build on in the future.


When I write these words, trying to think of this past year, I find it difficult not to think about the present. In the atrocities of the war, like in the tragedy of the pandemic, we see how solidarity brings us closer and helps us defeat the darkest hours.

Not by coincidence, solidarity is one of the main pillars of the [EDPS Strategy 2020-2024](#). I am proud that in 2021 our words were followed by actions. Our supervision of the EU institutions, agencies and bodies (EU institutions) is founded on a deep belief that high standards of legal compliance of EU public authorities is a necessary condition for their effectiveness. An efficient administration is an administration that respects the rule of law and acts on the basis of law, not around it.

The EDPS is committed to supporting the EU institutions in this endeavour. We note with satisfaction, as proven by remote inspections, guidelines and trainings, the overall high level of compliance with data protection principles regarding measures undertaken to combat the pandemic.

The [EDPS' Decision](#) to order Europol to delete datasets with no established links to criminal activity should also be seen in the context of our respect for the rule of law and mature checks and balances system. The EDPS wants strong EU institutions. This strength, however, can only be based on the full compliance with the mandate given to them by the EU legislator. No other foundation can bring results in the long term.

In the field of policy advice, amongst examples which can be found in the Annual Report 2021, our efforts can be seen in the Opinions



we delivered on a number of the EU legislators' initiative that have an impact on the protection of individuals' personal data, such as the [Digital Services Act](#) or the [Digital Markets Act](#). Our Opinions are based on the conviction that data generated in Europe is converted into value for European companies and individuals, and processed according to European values, to shape a safer digital future.

The EDPS has always been an institution that looks beyond the landscape of the EU institutions. We are committed to the success of the EU in the field of the fundamental rights to privacy and to data protection. Looking to the future, believing that the success of the GDPR is also our responsibility, we continued our active participation in the European Data Protection Board's work, as reflected in the number of initiatives we proposed or took part in.

Above everything else, we see the European Union as a community defined by values, not borders. For the EDPS, this belief is a motivation to further our efforts.

We hope that this belief will be shared more broadly across the European Union.

I dedicate the Annual Report 2021 to the EDPS staff whom I cannot thank enough for their work.



**Wojciech Wiewiórowski**

European Data Protection Supervisor



The background of the slide is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting various circular nodes of different sizes. The nodes and lines are more densely packed in the center and become sparser towards the edges, creating a sense of depth and connectivity.

# **MISSION, VALUES AND PRINCIPLES**

The work of the [European Data Protection Supervisor \(EDPS\)](#) is guided by its mission. Our core values and guiding principles inform this mission, as explained below.

## Mission statement

Data protection is a fundamental right, as enshrined in [Article 8](#) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the [Treaty on the Functioning of the European Union](#). Everyone has the right to the protection of personal data concerning them. This approach underscores our mission.

The EDPS is the European Union's (EU) independent supervisory authority with a number of responsibilities within its mission: monitoring the processing of personal data by the EU institutions, bodies, offices and agencies (EUIs); advising on policies and legislation that affect privacy; and cooperating with similar authorities to ensure consistent data protection. Its mission is also to raise awareness about risks, and to protect people's rights and freedoms when their personal data is processed.

[Regulation \(EU\) 2018/1725](#) outlines our tasks, powers and duties as an independent supervisor and impartial advisor on EU technologies, policies and laws that could affect the rights to privacy and data protection.

According to the [General Data Protection Regulation](#) (GDPR), the EDPS is a member of the [European Data Protection Board](#) (EDPB). The EDPS also collaborates within the EDPB to ensure the consistent application of data protection laws across the EU and provides the EDPB with a Secretariat, which offers analytical, administrative and logistical support, as outlined in the EDPS-EDPB [Memorandum of Understanding](#).

## Core values

The following values inform how the EDPS functions and performs its tasks.

- Impartiality - working within our legislative and policy framework, being independent and objective, finding the right balance between the interests at stake.
- Integrity - upholding the highest standards of behaviour and doing

what is right even if it is unpopular.

- Transparency - explaining what we are doing and why, in a clear language that is accessible to all.
- Pragmatism - understanding our stakeholders' needs and seeking solutions that work in practice.

## Guiding principles

The following principles guide the EDPS' work and interaction with stakeholders. Using our expertise, authority and formal powers, we:

- serve the public interest to ensure that EU institutions comply with data protection principles in practice;
- build awareness of data protection as a fundamental right, and as a vital part of public policy and administration for EU institutions;
- focus our attention and efforts on areas of policy or administration that present the highest risk of non-compliance or the greatest impact on privacy by acting selectively and proportionately.



The background of the slide is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting numerous small, light blue circular nodes. These nodes and lines are scattered across the entire frame, creating a sense of a global or digital network. The lines vary in length and orientation, forming a web-like structure.

# **EDPS STRATEGY 2020-2024**

On 30 June 2020, the EDPS presented its 2020-2024 Strategy '[Shaping a Safer Digital Future](#)' to the public.

The strategy was adopted amidst the [COVID-19 pandemic](#), which elevated the importance of the digital economy, as well as the need for effective guarantees concerning data protection and privacy.

### **About the Strategy**

The aim of the EDPS strategy is to shape a safer, fairer and more sustainable digital Europe, particularly for the most vulnerable in our societies. In the spirit of collaboration and unity, the EDPS will continue to work with authorities and experts across different policy areas to address the digital challenges of this new decade.

There are three core pillars to the EDPS strategy, which outline the guiding actions and objectives for the organisation from 2020 to the end of 2024.

**Foresight:** the EDPS' commitment to being a smart institution that takes the long-term view of trends in data protection and the relevant legal, societal and technological contexts.

**Action:** the EDPS proactively develops tools for EU institutions to be world leaders in data protection. We aim to promote coherence in the activities of enforcement bodies in the EU with a stronger expression of genuine European solidarity, burden sharing and a common approach.

**Solidarity:** the EDPS believes that justice requires privacy to be safeguarded for everyone, in all EU policies, while sustainability should be the driver for data processing in the public interest.



The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting small, semi-transparent blue dots. These dots and lines are scattered across the page, creating a sense of a digital or molecular structure. The lines and dots are more concentrated in the upper left and lower right areas, with some sparser regions in the center.

## **CHAPTER ONE**

# **An introduction to the EDPS**



## 1.1.

# About the EDPS

The [European Data Protection Supervisor](#) (EDPS) ensures that the European Union's institutions, offices, bodies and agencies (EUIs) respect the fundamental rights to privacy and data protection, whether they process personal data or develop new policies with an impact on the protection of individuals' rights and freedoms related to the processing of personal data. The EDPS has four main fields of work:

**Supervision:** We monitor the processing of personal data by the EU administration and ensure that they comply with data protection rules. Our tasks range from conducting investigations to handling complaints and prior consultations on processing operations.

**Consultation:** We advise the European Commission, the European Parliament and the Council on proposals for new legislation and other initiatives related to data protection.

**Technology monitoring:** We monitor and assess technological developments, where they have an impact on the protection of personal data, from an early stage, with a particular focus on the development of information and communication technologies.

**Cooperation:** We work with national data protection authorities (DPAs) to promote consistent data protection across the EU. Our main platform for cooperation with DPAs is the [European Data Protection Board](#) (EDPB), for which we also provide the secretariat.

[Regulation \(EU\) 2018/1725](#) is the EUIs equivalent to the [General Data Protection Regulation](#) (GDPR). The GDPR became fully applicable across the EU on 25 May 2018 and sets out the data protection rules with which all private and the large majority of public organisations operating in the EU must comply. It also tasks the EDPS with providing the secretariat for the EDPB.

In 2021, the EDPS prepared a detailed [contribution](#) on the application of Regulation (EU) 2018/1725 that the Commission has to present by 30 April 2022.



The processing of personal data by EU Member States' law enforcement authorities is governed by [Directive \(EU\) 2016/680](#) on data protection in the police and criminal justice sectors. [Article 3](#) and [Chapter IX](#) of Regulation (EU) 2018/1725 apply to the processing of operational personal data by EUIs involved in police and judicial cooperation, and these provisions are closely modelled on the rules set out in Directive 2016/680.

In addition, specific rules exist concerning the processing of personal data for operational activities carried out by:

- the EU law enforcement agency, [Europol](#), under [Regulation \(EU\) 2016/794](#);
- the EU agency for judicial cooperation, [Eurojust](#), under [Regulation \(EU\) 2018/1727](#);
- the European Public Prosecutor's Office ([EPPO](#)), under [Regulation \(EU\) 2017/1939](#);
- the European Border and Coast Guard ([Frontex](#)), under [Regulation \(EU\) 2019/1896](#).

As for the other EUIs, the EDPS is also responsible for supervising the processing of personal data relating to administrative activities in the aforementioned agencies, including personal data relating to their staff members, under Regulation (EU) 2018/1725.

## 1.2.

# Supervision and Enforcement

In our role as the data protection authority of EUIs, we aim to ensure that EUIs are not only aware of their data protection obligations, but are also held accountable for complying with them. We have several tools we can use, all of which are aimed at ensuring compliance with the Regulation, while encouraging the development of a data protection culture within the EUIs.

**Prior Consultations:** EUIs are required, in certain cases, to consult us after carrying out a Data Protection Impact Assessment ([DPIA](#)) for the intended processing of personal data which will result in a high risk to the rights and freedoms of individuals.

**Complaints:** We handle complaints from individuals relating to the processing of personal data by the EUIs. We investigate these complaints and decide on the best way to address identified issues, which includes using our corrective powers.

**Monitoring compliance:** We are responsible for ensuring that all EUIs, notably those involved in police and judicial cooperation matters (e.g., Eurojust, Europol and EPPO), comply with data protection rules, due to the high risk to the rights and freedoms of individuals. We monitor compliance in various ways, including through visits, [audits](#) and [investigations](#) of potential data protection infringements.

**Consultations:** We issue [Opinions](#) on administrative measures relating to the processing of personal data as well as Opinions on any issue concerning the protection of personal data, either in response to a specific request from an EUI, or on our own initiative.

**Guidance:** We issue [Guidelines](#) for the EUIs designed to help them better implement data protection principles and comply with data protection rules.

**Working with data protection officers (DPOs):** Each EUI must appoint a DPO, who is responsible for reinforcing the accountability principle by assisting their EUI to comply with data protection rules. We work closely with these DPOs, providing them with training and support to help them perform their role effectively.

**Training the EUIs:** We provide general and thematic training sessions for managers and staff members of the EUIs. These help to ensure compliance with data protection rules and respect for the rights and freedoms of individuals and to encourage the development of a data protection culture within each EUI. These training sessions focus on helping EUIs to go beyond compliance and demonstrate accountability.

[See Chapter 3: Supervision and Enforcement](#) and [Chapter 4: Supervising the Area of Freedom, Security and Justice](#).

### 1.3.

## Policy and Consultation

**Legislative consultation:** The EDPS acts as an adviser to the EU legislator on data protection issues. We aim to ensure that data protection requirements are integrated into all new legislation, policy initiatives and international agreements. This is done by providing guidance on proposed legislation to the European Commission, as the institution with the right of legislative initiative, and the European Parliament and the Council, as co-legislators.

Our guidance may take different forms, detailed below.

**Opinions:** Our Opinions are issued in response to mandatory requests by the European Commission which is legally obliged to seek our guidance on any legislative proposal, or draft Implementing Act/Delegated Act, as well as recommendations and proposals to the Council in the context of international agreements according to [Article 42\(1\)](#) of Regulation (EU) 2018/1725.

Opinions, as well as their summaries in all official languages of the EU, are available on the EDPS website and published in the [Official Journal of the EU](#). Opinions highlight our main data protection concerns and recommendations on legislative proposals or other measures. They are issued in response to a request from the European Commission and are addressed to the EU co-legislator. A complete list of the EDPS' 2021 Opinions can be found in [Annex D. See section 6.2: A selection of significant and important Opinions.](#)

**Formal Comments:** Similar to our Opinions, our Formal Comments are issued in response to a request from the European Commission under Article 42(1) and address the data protection implications of legislative proposals. However, they are usually shorter and more technical, or only address certain aspects of a proposal. Our Formal Comments are published on our website. A complete list of the EDPS' 2021 Formal Comments can be found in [Annex E. See section 6.4: A selection of significant and important Formal Comments.](#)

**Informal Comments:** The European Commission is encouraged to consult us informally before adopting a proposal which has an impact on

data protection. This allows us to provide the European Commission with input at an early stage of the legislative process, usually at the stage of the inter-service consultation. Informal Comments are, in principle, not published.

**Joint EDPS-EDPB Opinions:** Where a legislative or other relevant proposal is of particular importance for the protection of personal data, the European Commission may also consult the EDPB. In such cases, the EDPS and the EDPB work together to issue a Joint Opinion ([see section 6.3: An overview of the most significant and important Joint Opinions](#)).

Beyond mandatory legislative consultations, we also have the power to issue Opinions on any issue of relevance to the protection of personal data, addressed to the EU legislator or to the general public, in response to a consultation by another institution or on his own initiative.

**International Cooperation, including with national DPAs:** In addition to being a member of the EDPB, we cooperate with international organisations to promote a data protection culture. In this context, we have been organising workshops on data protection with International Organisations, since 2005. We are also an active member of the Global Privacy Assembly ([see Chapter 8: International Cooperation](#)).

**Court Cases:** We can intervene and offer our data protection expertise before the EU Courts, either through interventions in support of one of the parties in a case, or at the invitation of the Court.

1.4.

## Technology and Privacy

The EDPS monitors technological developments and their impact on data protection and privacy. Knowledge and expertise in this area allow us to effectively perform our supervision and consultation tasks. This capacity and competence will only continue to grow in importance due to the rapid changes in technology and the accelerated pace of digital transformation in the EU and in the EUIs.

Our activities include:

Monitoring and responding to technological developments: We monitor technological developments, events and incidents and assess their impact on data protection. This allows us to provide advice on technology choices, e.g. in the context of working on digital sovereignty, and on technical matters, particularly in relation to the EDPS' supervision and consultation tasks.

**Promoting privacy engineering:** In 2014, we launched the [Internet Privacy Engineering Network](#) (IPEN) in collaboration with national DPAs, developers and researchers from industry and academia, and civil society representatives. Our aim is to both develop engineering practices that incorporate privacy concerns and to encourage engineers to build privacy mechanisms into internet services, standards and apps.


**Establishing the state of the art in data protection by design:** With the GDPR and Regulation (EU) 2018/1725 now fully applicable, it has become a legal obligation for all data controllers to take account of the state of the art in data protection friendly technology when designing, maintaining and operating IT systems for the processing of personal data. In order to ensure consistent application of this rule across the entire EU, DPAs must work together to establish a common understanding of the state of the art and its development.



The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract geometric pattern. It consists of numerous thin, light blue lines that connect various points. These points are represented by small, semi-transparent blue dots of varying sizes. The pattern is dense and irregular, resembling a network or a molecular structure. The lines and dots are more concentrated in the upper left and lower right areas, with some sparser regions in the center.

## **CHAPTER TWO**

# **2021 HIGHLIGHTS**



This chapter presents the main activities and achievements of the EDPS in 2021.

## 2.1.

# International transfers of personal data

Following the Court of Justice of the European Union's [Schrems II judgment](#), the EDPS pursued and launched various activities and initiatives in the framework of the EDPS' Strategy for EU institutions, bodies, offices and agencies (EUIs) to comply with the "Schrems II" judgment ([EDPS' Schrems II Strategy](#)), published on 29 October 2020.

The strategy aims to ensure and monitor the compliance of EUIs with the judgment concerning transfers of personal data outside the EU and the European Economic Area (EEA), in particular the United States of America. As part of the strategy, we are pursuing three types of actions: investigations; authorisations and advisory work; and general guidance to assist the institutions in discharging their duty of accountability.

Notably, in May 2021, we launched [two investigations](#): one on the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EUIs, and one on the use of Microsoft Office 365 by the European Commission. With these investigations, the EDPS aims to help EUIs improve their data protection compliance when negotiating contracts with their service provider.

In addition, we issued a number of decisions on transfers of personal data to non-EU/EEA countries. Our decisions are based on assessing whether the tools that the EUI in question envisages to use to transfer personal data outside of the EU/EEA affords an essentially equivalent level of protection for individuals' personal data as in the EU/EEA.

To find out more about the EDPS' work on transfers of personal data, read [Chapter 3 part 1: Transfers of personal data to non-EU/EEA countries](#), and [Chapter 3 part 6: EDPS investigations](#).



## 2.2.

# COVID-19 and data protection, our efforts continue

Throughout 2021, the EDPS continued to monitor the COVID-19 pandemic and its impact on data protection through its dedicated [COVID-19 task force](#), initially set up in 2020. As the data protection authority of EUIs and as an employer itself, we produced guidelines, and other initiatives to support EUIs in their processing activities during this time.

As EUIs developed strategies for their return to the office, we published guidelines on 9 August 2021 titled, [Return to the Workplace and EUIs' screening of COVID immunity or infection status](#). Our guidelines include recommendations on a variety of matters, such as EUIs' possible use of COVID antigen test results, the use of employees' vaccination status and EU COVID certificates.

The dynamic evolution of the COVID-19 pandemic means that EUIs must continually adapt their processes. As such, we conducted a [survey](#) asking all EUIs about how they have changed or developed new processing operations due to COVID-19. The survey included question on EUIs' new processing operations; IT tools EUIs put in place or enhanced to enable teleworking; and new processing operations put in place by EUIs in charge of tasks related to public health. The results of the survey, shared with the data protection officers of EUIs and later on with the public, will feed into updating existing EDPS guidelines, or contribute to the development of new guidelines, depending on the evolution of the pandemic and the new practices that will continue once it is over.

We also felt it was necessary to provide training on the use of social media, remote working tools and other ICT tools used by EUIs, due to the increase in the use of these tools to connect both internally and with their audience during COVID-19. During our training sessions, we emphasised that the use of social media and videoconference tools should be considered like any other ICT tools when assessing their data protection implications and adopting necessary measures to ensure that individuals' privacy is protected. Compliance with the EU's data protection framework in this context was regularly checked by the EDPS.

## 2.3.

# Supervising the Area of Freedom, Security and Justice

In 2021, the EDPS continued to supervise the bodies and agencies that are part of the Area of Freedom Security and Justice (AFSJ), which covers policy areas that range from the management of the European Union's external borders to the judicial cooperation in civil and criminal matters. The AFSJ also includes asylum and immigration policies, police cooperation and the fight against crime, such as terrorism; organised crime; trafficking of human beings; drugs.

## Supervising Europol

Some of our notable work in the Area of Freedom, Security and Justice, include our supervision activities regarding the processing of personal data by [Europol](#), the EU Agency for Law Enforcement Cooperation.

In particular, we supervised Europol over their use of machine learning tools, which we initially started in 2019. In line with our Strategy, our work focused, and continues to focus, on the use of operational data for the development, including training, testing, validation, and use of machine learning models for data science purposes. Our supervision work consisted of an own-initiative inquiry, followed by a prior consultation that we issued in February 2021, which led us to deliver an opinion of 21 recommendations that Europol should follow in order to avoid possible breaches of the Europol Regulation. Our Opinion suggested, in particular, that Europol establishes an internal governance framework to ensure that, in the course of developing machine learning models, Europol identifies the risks to fundamental rights and freedoms posed by the use of these innovative technologies, even if Europol might not always be in a position to mitigate all of them, on the basis of the current state-of-the-art. The development and use of such models was also one of the topics of Europol's Annual Inspection in September 2021. The inspection covered Europol's machine learning tool development process and the related data protection risk assessment process.

Another important part of our work in 2021 concerned our inquiry into Europol's processing of large datasets, initially launched in 2019. In December 2021, we decided to use our corrective powers by issuing

an [order](#) - formally communicated to Europol on 3 January 2022 - to delete data concerning individuals with no established link to a criminal activity (Data Subject Categorisation). More specifically, we impose a 6-month retention period for Europol to filter and to extract the personal data and a 12-month period to comply with the EDPS Decision. This Decision comes after the EDPS admonished Europol in September 2020 for the continued storage of large volumes of data with no Data Subject Categorisation, which poses a risk to individuals' fundamental rights.

### Supervising Eurojust

In 2021, the EDPS continued to work closely with the DPO and other operational staff of [Eurojust](#), the European Union Agency for Criminal Justice Cooperation, by providing them with informal advice when needed.


Following the adoption of the [EU-UK Trade and Cooperation Agreement](#), we contributed to the fine-tuning of Eurojust's relations with competent UK authorities. The EDPS provided advice on practical data protection questions and delivered opinions on the working arrangements between Eurojust and the UK's Home Office.

Our first data protection audit of Eurojust's data protection activities, initially scheduled for 2020 and postponed due to the pandemic, took place in October 2021. The EDPS' audit focused on the processing of operational personal data by Eurojust and looked at data transfers in Eurojust's external relations; the functioning of the counter terrorism register and data security; and the use and performance of Eurojust's Case Management System, in particular. Following the onsite visit of the EDPS as part of the audit, we found that, overall; Eurojust's compliance with the data protection framework was satisfactory, with no critical compliance issues.

### Supervising EPPO

The European Public Prosecutor's Office ([EPPO](#)), the independent European body with the power to investigate and prosecute criminal offences against the EU's financial interests, became operational in June 2021.

To this end, our work and efforts in 2021 focused on supporting EPPO to establish itself before it became operational. For an effective collaboration,



the Supervisor of the EDPS met with the European Chief Prosecutor, Ms Laura Kövesi, to discuss their ongoing and future cooperation.

### Supervising Frontex

In 2021, we also supported the activities of [Frontex](#), the European Border Coast Guard Agency, which contributes to the effective management of European borders.

We provided guidance on Frontex's activities in assisting EU Member States when returning migrants - who do not fulfil the conditions to stay in the EU - are sent back to their home country. In particular, we gave our advice on the technical tools Frontex and EU Member States are using in this context, and provided [advice](#) on the transfers of personal data about these migrants by Frontex to non-EU countries.

To find out more about the EDPS' work in the Area of Freedom, Security and Justice, read [Chapter 4: The Supervision of the Area of Freedom, Security and Justice](#).

## 2.4.

# Shaping Europe's Digital Future

As set out in our [EDPS Strategy 2020-2024](#), we value initiatives where data generated in Europe is converted into value for European companies and individuals, and processed in accordance with European values, to shape a safer digital future. Amongst other examples, which can be found in the Annual Report 2021, our efforts can be seen in the Opinions we delivered on a number of the EU legislators' initiative having an impact on the protection of individuals' personal data.

### The Digital Markets Act and Digital Services Act

In February 2021, the EDPS published two Opinions, one on the EU's [Digital Markets Act](#) and one on the EU's [Digital Services Act](#).

We welcomed the proposal for a Digital Services Act that seeks to promote a transparent and safe online environment. We recommended that additional measures are put in place to better protect individuals when it comes to content moderation, online targeted advertising and

recommender systems used by online platforms, such as social media and marketplaces.

Concerning the Digital Markets Act, 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.

### Artificial Intelligence

In June 2021, with the European Data Protection Board (EDPB), we issued a [Joint Opinion](#) on the European Commission's Proposal on the Artificial Intelligence Act. With individuals' privacy rights and safety in mind, we called for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces.

### The EU's Cybersecurity Strategy

In March 2021, we issued an Opinion on the EU legislator's [Proposal for the NIS 2.0 Directive](#), which aims to replace the existing Directive on security of network and information systems (NIS) and is part of the EU's Cybersecurity Strategy. In our Opinion, we underlined that it is essential that privacy and data protection are embedded in the proposed Directive and in all future initiatives stemming from the EU's Cybersecurity Strategy. This will allow for a holistic approach when managing cybersecurity risks and protecting individuals' personal data.

### The Digital Green Certificate

In April 2021, together with the EDPB, we adopted a [Joint Opinion on the Proposals for a Digital Green Certificate](#). The Digital Green Certificate aims to facilitate the exercise of the right to free movement within the EU during the COVID-19 pandemic by establishing a common framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, testing and recovery certificates.

With this Joint Opinion, we invited the co-legislators to ensure that the Digital Green Certificate is fully in line with EU personal data protection legislation. Our Joint Opinion underlined that the use of the Digital Green Certificate may not, in any way, result in direct or indirect discrimination of individuals, and must be fully in line with the fundamental principles of necessity, proportionality and effectiveness.



## 2.5.

# An increase in legislative consultations

Since the entry into application of the data protection regulation for EUIs, [Regulation \(EU\) 2018/1725](#), the number of legislative consultations has increased significantly.

In 2021, the EDPS responded to 88 Formal Legislative Consultations, compared to 27 in 2020. The 88 legislative consultations include 12 Opinions and 76 Formal Comments, in addition to 5 Joint Opinions issued with the EDPB.

This steep increase can be explained by several factors.


There has been a greater number of legislative initiatives containing provisions that have an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data. Therefore, more EU institutions and organisations have contacted the EDPS for legislative consultation.

This increase is also due to the strengthening of the EDPS' consultative role under [Article 42](#) of Regulation (EU) 2018/1725, which establishes a clear positive obligation for the European Commission to consult us on legislative proposals and other proposals with an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.

Amongst other factors, there is a growing awareness of data protection issues within the European Commission's departments. This awareness raising is due to both the outreach undertaken by the EDPS, and clarifications made internally by the European Commission.

In 2021, a series of significant EDPS Opinions have been issued on three themes in particular: digital platforms, financial services and justice and home affairs.

Our Joint Opinions with the EDPB include the topics of Artificial Intelligence, the Digital Green Certificate, Standard Contractual Clauses, to name a few examples.



Our key Formal Comments issued in 2021 concern, amongst others, Justice and Home Affairs and the European Health Union Package.

To find out more about the EDPS' Legislative Consultation of the year 2021, read [Chapter 6: Legislative Consultations](#).

2.6.

## Pleadings before the Court of Justice of the European Union

Throughout 2021, the EDPS participated in four hearings before the Court of Justice of the European Union (CJEU) concerning different matters. Our interventions in cases that are pending before the CJEU is one of the tangible ways we fulfil our advisory role. In our interventions, we can highlight specific data protection issues to ensure that individuals' fundamental rights to privacy and data protection are respected.

### Passenger Name Records

In July 2021, the EDPS replied to written questions by the CJEU and participated in an oral hearing in a case concerning the validity and interpretation of the [EU Directive 2016/681](#) on the use of passenger name record data (PNR) - which includes passengers' booking details when travelling - for the prevention, detection, investigation and prosecution of terrorist offences and serious crime ([Case C-817/19](#)).

The claimant before the Belgian Constitutional Court which referred the case, the Ligue des droits humains, a Belgian non-governmental organisation, claimed that the Belgium PNR Law, which transposed the PNR Directive, unlawfully interfered with individuals' right to privacy and right to the protection of their personal data. The claimant considered, in particular, that the processing operations of individuals' data that it entailed was not necessary and proportionate in light of the criteria set out in data protection law.

During the hearing, the EDPS stressed the need for effective safeguards to mitigate the risks stemming from the processing of PNR data, bearing in mind its large-scale, systematic and intrusive nature. The EDPS also expressed doubts about the compatibility of the processing of PNR data from intra-EU flights and from other intra-EU cross-border means of public



transport with the Treaties and [the EU Charter of Fundamental Rights](#).

### Data retention

In September 2021, the EDPS participated in two CJEU hearings in cases concerning data retention.

The first hearing addressed the compatibility of German and Irish laws on retention of personal data for law enforcement purposes with Article 15 of the [ePrivacy directive](#), which governs restrictions of individuals' rights to privacy and to the protection of personal data in electronic communications (C-793/19, C-794/19 and C-140/20).

During the hearing, the EDPS reiterated that it might be possible to envisage clear and precise legislation providing for a limited but effective regime for the retention and access to traffic and location data of electronic communications, including data of users that at first sight have no objective connection with the objective pursued, in a manner compatible with the EU Charter of Fundamental Rights, and that retention and access to stored data should not be considered in watertight isolation from each other.

The second hearing concerned two French cases related to the use of data retention to investigate insider dealings and market manipulations under the [EU's Market Abuse Directive](#) and [Market Abuse Regulation](#) (C-339/20 and C-397/20). One of the issues in question was whether this legislation allows the national legislator to require general retention of personal data to enable competent authorities to access this data when investigating insider dealings and market manipulations.

At the hearing, the EDPS took the view that these provisions did not aim at establishing a data retention legal basis.

### Anti-money laundering

In October 2021, the EDPS took part in a CJEU hearing in a case concerning [EU Directive 2018/843](#) on the prevention of money laundering and terrorist financing (C-601/20). Specifically, the hearing focused on how to interpret the relevant provisions of this EU Directive concerning the regime of public access to information on beneficial ownership and whether this interpretation complies with the EU Charter of Fundamental Rights and the General Data Protection Regulation.



In line with our [Opinion](#) on anti-money laundering published in September 2021, we argued that access of the general public to information on beneficial ownership, as set out in the Directive is not necessary and proportionate.

2.7.

## A new initiative, TechSonar

One of the EDPS' achievements of the year 2021 was the launch of a new initiative, [TechSonar](#), in September.

With our TechSonar report, we aim to anticipate emerging technology trends to better understand their future developments, especially their potential implications on data protection and individuals' privacy.

This new initiative comes after some reflections within the EDPS. The COVID-19 pandemic, amongst other factors, has accelerated technological change, with the appearance of new technologies and tools. Often, we do not know the real main uses that these technologies will have until they are applied in specific contexts. It is only then that we are able to understand the value and risks that these technologies may have on society. To this end, the EDPS firmly believes that it is necessary to act in advance, meaning that, instead of reacting to new emerging technologies when their added value and risks for society are already developed, we should be able to anticipate their developments. This would allow us to ensure that these technologies are developed, from the earliest stages of their conception, according to individuals' fundamental rights, including the rights to privacy and data protection.

In light of this, TechSonar is a process that aims to empower the EDPS to continuously analyse the technology arena with the aim of selecting tech trends we foresee for the following year.

With TechSonar, we are able, and will continue, to determine which technologies are worth monitoring today in order to be prepared for a more sustainable digital future where the protection of personal data is efficiently guaranteed.

In our first 2021 TechSonar report, our team of in-house experts chose to explore the following six foreseen technology trends: Smart vaccination

certificates; Synthetic data; Central bank digital currency; Just walk out technology; Biometric continuous authentication; Digital therapeutics.

To find out more about TechSonar and the EDPS' work in the area of technology and privacy, read [Chapter 5: Technology and Privacy](#).

2.8.

## Human Resources, Budget and Administration

Throughout 2021, the EDPS' Human Resources, Budget and Administration Unit (HRBA) has provided support to the Management and Operational teams of the EDPS. The aim is to ensure that they have sufficient financial, human and administrative resources and tools to achieve the goals set out in the [EDPS Strategy 2020-2024](#).

### Managing the COVID-19 pandemic

Amongst the work and initiatives pursued in 2021, the HRBA unit put in place an internal strategy for a gradual and safe return to the EDPS' premises, aligned with the Belgian's COVID-19 measures and the measures adopted by the other EUIs. As such, HRBA orchestrated the return to the EDPS offices in phases over the course of the pandemic, with specific working arrangements and health and safety rules.

### Well-being at work

As an organisation, we focus on creating a positive impact in our society. One of our core values is to treat individuals, including our staff, with respect. To build a positive, respectful and safe working environment, HRBA continued a number of initiatives, already started in 2021, to ensure high levels of well-being at work amongst EDPS staff, by working closely with the EDPS' Well-being Coordinator.

### Recruiting data protection experts

One of the priorities set out in our EDPS Strategy 2020-2024 is to invest in knowledge management to ensure the highest quality of our work and to recruit a diverse, inter-disciplinary and talented workforce. As such, in 2021, we concentrated our efforts to recruit data protection experts to meet the EDPS' needs.



### Adapting our working conditions

The changes in our working environment caused by the pandemic and the full-time teleworking regime called for a deep reflection on the adaptation of our working conditions. We considered factors including working time, hybrid working and telework from abroad. The HRBA unit began this reflection and will propose new rules, which will be discussed and agreed upon by our staff committee. The aim is to adopt these rules by mid - 2022.

### Looking forward: creating the European House of Data Protection

The EDPS and the EDPB became the sole occupants of its current premises in Brussels following the departure of the European Ombudsman at the end of October 2021. This paved the way for us to start creating and establishing our premises as “The European House of Data Protection”, with the aim to become the EU’s Brussels-based hub for privacy and data protection. This project started in 2021 and will continue throughout 2022.

To find out more, read [Chapter 12: Human Resources, Budget and Administration](#)

## 2.9.

## The EDPS’ Communication Activities

Public interest in and engagement with data protection and the work of data protection authorities (DPAs) continues to grow, 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 Sector (I&C Sector) aims to, therefore, ensure that EDPS activities and messages reach the relevant audiences at the right time.

The role of the I&C Sector, reinforced in the [EDPS Strategy 2020-2024](#), is to explain and promote the work of the EDPS. This commits 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’ day-to-day work in clear language and via appropriate communication tools.

To this end, our work in 2021 focused on developing and modernising the

EDPS' visual identity. With our new corporate identity, we aim to reflect the role of the EDPS as a global leader in data protection and privacy not only in the EU, but also beyond, and to mark a new era in the history of the EDPS, which will focus more on shaping a safer digital future.

A large part of I&C's time and effort is invested in promoting the EDPS' activities on our three well-established social media channels: [Twitter](#), [LinkedIn](#), and [YouTube](#). This may include developing social media campaigns centred on specific themes, promoting the Supervisor's participation at important events, and more. We have also continued to produce and publish content on the EDPS Website. This includes the publication of Factsheets, our ever-growing Newsletter, blogposts on an array of subject matters, and EDPS press releases, to name a few examples.

To find out more, read [Chapter 11: The EDPS' Communication Activities](#).

## 2.10.

# Key Performance Indicators

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 2021. These results are measured against initial targets, or against the results of the previous year, used as an indicator. This set of KPIs were partly revised at the end of 2020, to ensure that the performance metrics adapt to developments in EDPS activities.

In 2021, we met or surpassed - in some cases significantly - the targets set in eight out of nine KPIs, with one KPI, KPI8 on the occupancy rate of the establishment plan, just falling short of the set target.

These results clearly illustrate the positive outcome we have had in implementing our strategic objectives throughout the year, notwithstanding the challenging circumstances in which the EDPS still had to operate in the context of the COVID-19 Pandemic.

KEY PERFORMANCE INDICATORS		RESULTS 31.12.2021	TARGET 2021
KPI 1 Internal indicator	Number of initiatives, including publications, on technology monitoring and on promoting technologies to enhance privacy and data protection organised or co-organised by the EDPS	16 initiatives	10 initiatives
KPI 2 Internal & External Indicator	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8 activities	8 activities
KPI 3 Internal Indicator	Number of cases dealt with in the context of international cooperation (GPA, CoE, OECD, GPEN, Spring Conference, international organisations) for which the EDPS has provided a substantial written contribution	17 cases	5 cases
KPI 4 External Indicator	Number of files for which the EDPS acted as a lead rapporteur, rapporteur, or a member of the drafting team in the context of the EDPB	23 cases	5 cases
KPI 5 External Indicator	Number of Article 42 Opinions and Joint EDPS-EDPB Opinions issued in response to the European Commission's legislative consultation requests	17	Previous year as benchmark
KPI 6 External Indicator	Number of audits/visits carried out physically or remotely	4 audits + 1 visit 43 EUIs impacted	3 different audits/visits 30 EUIs impacted
KPI 7 External Indicator	Number of followers on the EDPS social media accounts	Twitter: 25826 LinkedIn: 49575 YouTube: 2438	Results of previous year + 10%
KPI 8 Internal Indicator	Occupancy rate of establishment plan	88%	90%
KPI 9 Internal Indicator	Budget implementation	86,12%	80%

Figure 1: Key Performance Indicators

The background is a dark blue gradient with a complex network of thin, light blue lines connecting small, semi-transparent blue dots. These dots and lines are scattered across the entire page, creating a sense of a digital or interconnected space.

## **CHAPTER THREE**

# **Supervision and Enforcement**



### 3.1.

## Transfers of personal data to non-EU/EEA countries

Following the Court of Justice of the European Union's [Schrems II judgment](#), we pursued and launched various activities and initiatives in the framework of the EDPS' Strategy for EU institutions, bodies, offices and agencies (EUIs) to comply with the "Schrems II" judgment ([EDPS' Schrems II Strategy](#)), published on 29 October 2020.

The strategy aims to ensure and monitor compliance of EUIs with the judgment concerning transfers of personal data to non-EU/EEA countries and in particular, the United States of America (USA). As part of the strategy, the EDPS is pursuing three types of actions: investigations; authorisations and advisory work; and general guidance to assist the institutions in discharging their duty of accountability.

### 3.1.1.

## EDPS investigations on Schrems II

Following the publication of the EDPS' Schrems II Strategy, we [launched two investigations](#) on 27 May 2021. These investigations aim to ensure that any ongoing and future international transfers by EUIs, or on EUIs' behalf, are carried out according to EU data protection law.


The first investigation focuses on the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EUIs, while the other investigation focuses on the use of Microsoft Office 365 by the European Commission.

[See 3.6: Investigations](#)

### 3.1.2.

## EDPS decisions on international transfers of data

In 2021, the EDPS issued four decisions on transfers of personal data



from EUIs to non-EU organisations. We issued these decisions based on the tools that the EUIs in question have envisaged to use to transfer personal data. As such, the focus of our decisions were on administrative arrangements and contractual clauses for transfers of personal data.

## 1. Authorisation of administrative arrangements to transfer personal data

### 1A. Data transfers between the Commission and the Turkish Medicines and Medical Devices Agency

On 12 May 2021, we issued our first [Decision](#) on the use of an administrative arrangement as a tool providing appropriate safeguards for the transfer of individuals' personal data to non-EU/EEA countries.

The arrangement focuses on transfers of individuals' personal data between the European Commission and the [Turkish Medicines and Medical Devices Agency](#) (TMMDA) in the context of the Turkish participation in the EU regulatory system for medical devices [EUDAMED](#).


The assessment was based on the European Data Protection Board's [Guidelines](#) (EDPB) for transfers of personal data between EEA and non-EEA public authorities and bodies, as these guidelines explain the criteria of the minimum data protection safeguards for such transfers.

To issue the Decision, we assessed whether the arrangement ensures that individuals' personal data transferred outside the EU/EEA is essentially equivalent to the level of protection as in the EU/EEA.

We considered the following principles as particularly important to provide sufficient data protection safeguards:

- purpose limitation - the transfer of individuals' data is limited to one specific purpose;
- data accuracy - to ensure that data collected is accurate and up to date;
- data minimisation - collection of an individual's personal data should be limited to what is necessary;
- storage limitation - an individual's data cannot be kept for longer than is necessary.





As a result, we recommended in the Decision that the European Commission should amend the following clauses to ensure that individuals' data is appropriately safeguarded:

- the purpose for which individuals' data may be processed;
- transparent information on how, what, why and how long individuals' data may be processed;
- information for individuals on their data protection rights;
- security and confidentiality measures for when individuals' data may be processed;
- redress, meaning the available options for individuals in case their data is not adequately protected;
- oversight of the processing operations of individuals' personal data.

Concerning the possible access to individuals' personal data by national security or law enforcement authorities, we reiterated that the Commission - as data exporter - is responsible for seeking and assessing whether the authorities in Turkey - as data importer - provide sufficient data protection safeguards. We also advised the Commission to keep records of the laws in force in Turkey that govern the sharing of personal data with other public bodies, including for surveillance purposes. These records should be communicated to us, within six months after the date of the EDPS Decision.

As is the process for all our decisions, we asked the European Commission to report on an annual basis on how the implementation of the Decision issued is going and to inform the EDPS without delay of any suspended transfers of data, or in the event of a revision or termination of the administrative arrangement with the TMMDA.

### 1B. Transfers of medical and health data

On 17 June 2021, we issued a Decision authorising, subject to conditions, the use of an administrative arrangement between the European Medicines Agency and the Department of Health of Canada concerning the exchange of personal data in their capacity as regulators and public authorities responsible for the supervision and pharmacovigilance of medicinal products.

## 1C. Transfers of personal data to the ITER International Fusion Energy Organisation

We issued another Decision on 5 July 2021 authorising, subject to conditions, the use of an administrative arrangement between the [European Joint Undertaking for ITER and the Development of Fusion Energy](#) and the ITER International Fusion Energy Organisation in the wider context of the implementation of the ITER Agreement.

### 2. Authorisation of contractual clauses to transfer personal data

On 31 August 2021, we issued a [decision](#) following a request from the Court of Justice of the European Union for the authorisation of ad-hoc contractual clauses between the Court, Cisco International Limited UK and Cisco Systems Inc. in the context of transfers of personal data in the Court's use of Cisco Webex and related services.

The EDPS authorised the use of ad hoc contractual clauses between the Court and Cisco until 30 September 2022.

In our findings, we identified several compliance issues with the draft ad-hoc contractual clauses submitted to us. After their submission, the Court and Cisco had put in place additional measures and made mutual commitments to take even further specific measures, such as limiting data transfers outside the EU and concrete encryption, which we also assessed and considered in our decision.

We imposed a number of conditions that the Court and Cisco are required to put in place to ensure compliance with [Regulation \(EU\) 2018/1725](#) and to ensure the essentially equivalent level of protection for transferred data. Conditions include:

- locating processing within the EEA;
- concluding additional contractual safeguards;
- measures for the effective encryption of data processed in the EEA;
- measures for the effective pseudonymisation or anonymisation of the remaining personal data processed outside the EEA, including through any remote access.

The Court must resolve the compliance issues identified within one year from the date of the decision, following which we will reassess the transfer authorisation and may order the suspension of data flows. The Court should also provide an intermediary report within six months of the decision date, which demonstrates that the conditions included in its decision are being put in place.

### 3.1.3.

## Data Protection Impact Assessments for data transfers


On 7 July 2021, we issued an Opinion following a prior consultation request from the European Central Bank (ECB) on its data protection impact assessment (DPIA) concerning a new Customer Relationship Management system for the ECB, based on Microsoft Dynamics 365.

In our Opinion, we addressed whether mitigating measures identified by the ECB in its DPIA were sufficient to appropriately address the high risks identified by the ECB in relation to its use of Microsoft Dynamics 365; this included:

- non-compliance with the rules on international transfers in light of the Schrems II Judgment;
- lack of control over Microsoft sub-processors;
- certain limitations of the contract with Microsoft negotiated by the European Commission on behalf of all EUIs.

We concluded that the measures envisaged by the ECB were insufficient to mitigate the high risks it had identified. We found that there were no sufficient guarantees and appropriate safeguards that the processing and transfers of personal data to Microsoft and its sub-processors, in the ECB's use of Microsoft Dynamics 365, will meet the requirements of Regulation (EU) 2018/1725, and ensure an essentially equivalent level of protection to that guaranteed in the European Economic Area (the EEA).

We issued a warning and made several recommendations to assist the ECB in ensuring that the processing of personal data by the ECB,



Microsoft and any sub-processors is compliant.

To name a few examples, these recommendations focused on assessing new contractual data protection safeguards, on the technical and organisational measures to put in place concerning international transfers to Microsoft or its sub-processors, and on assessing alternative solutions to Microsoft Dynamics 365.

#### 3.1.4.

### Training EUI's staff on personal data transfers to non-EU/EEA countries


Over the course of 2021, EDPS staff gave a series of advanced lectures online at the European School of Administration (EUSA) and other venues for staff members of all EUIs and their DPOs concerning transfers of personal data by EUIs or on their behalf.

Two online training sessions were held this summer, one on transfers of personal data to non-EU/EEA public bodies and organisations; and the other on the conditions and data protection safeguards for transfers to non-EU/EEA private entities.

Transferring personal data to non-EU/EEA countries may present additional risks for individuals, as these countries may not have the same legislation put in place to ensure that personal data is adequately and sufficiently protected. This is why when transferring individuals' personal data to countries outside the EU/EEA, EUIs have to ensure that the level of protection offered by the country of destination offers an essentially equivalent level of protection as in the EU/EEA.

During the training sessions, EDPS colleagues gave recommendations on how EUIs may carry out Transfer Impact Assessments (TIA) and possible supplementary measures to put in place to ensure that the country of destination ensures the essentially equivalent level of data protection as in the EU/EEA. S&E colleagues emphasised that if no essentially equivalent level of protection is guaranteed by a country of destination, then the transfer of individuals' personal data to that country should not occur.

We regularly organise training sessions and lectures on challenging



topics, such as the topic of international data transfers, for EUIs, their data protection officers, and their members of staff. These training sessions, either organised on our own initiative, or at the DPO's request, aim to ensure that EUIs stay up to date with data protection regulation and requirements in their day-to-day activities.

### 3.2.

## COVID-19 and data protection, our efforts continue

Throughout 2021, we continued to monitor the COVID-19 situation and its impact on data protection through its dedicated COVID-19 [task force](#), initially set up in 2020. As the data protection authority of EUIs and as an employer itself, we produced guidelines, and other initiatives to support EUIs in their processing activities during this time.

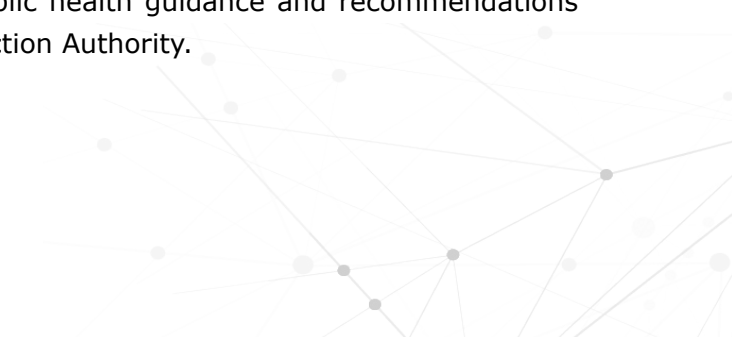
### 3.2.1.


## EDPS Guidelines for EUIs' return to the workplace

As EUIs developed strategies for their return to the office, we published guidelines on 9 August 2021 titled, [Return to the Workplace and EUIs' screening of COVID immunity or infection status](#).

The guidelines include recommendations on a variety of matters, such as EUIs' possible use of COVID antigen test results, the use of employees' vaccination status and EU COVID certificates.

Before putting in place these measures, we recommended that:

- EUIs carefully assess whether these measures would comply with the EU data protection law applicable to EUIs, Regulation (EU) 2018/1725, to minimise the intrusion into individuals' privacy;
  - the measures envisaged by EUIs are in line with the legislation of the EU Member State where the EUI in question is located, as well as that Member State's latest public health guidance and recommendations made by their Data Protection Authority.
- 



When it comes to employees' COVID antigen test results and COVID Certificates - which include employees' personal data – we recommended that the following two distinctions are made:

- if EUIs proceed to manual verifications of antigen test results and COVID certificates without further storing or registering this information, this would not qualify as personal data processing;
- if EUIs proceed to the verification of the antigen test results and COVID certificates by scanning QR codes or recording the results in a database for example, this would be considered as processing employees' health data. Health data is considered as a special category of data and requires extra protection.

In our Guidelines, we emphasised that when EUIs plan their employees' return to the office they should do so without intruding on employees' privacy, by selecting measures that demand the least amount of processing of employees' personal data. EUIs should also assess whether such processing of individuals' personal data is necessary and proportionate in light of the measures envisaged for a return to the workplace. The least intrusive measures should always be the preferred option to select.


### 3.2.2.


## EUIs' COVID-19 Survey

In 2021, we prepared a [report](#) on the new processing operations, and on the IT tools that EUIs introduced to ensure business continuity during the COVID-19 pandemic and the compliance of these activities with Regulation (EU) 2018/1725.

The report is based on an earlier survey and comprises three parts: new processing operations put in place by EUIs; IT tools put in place or enhanced by EUIs to enable teleworking; and new processing operations put in place by EUIs in charge of tasks related to public health.

The dynamic evolution of the COVID-19 pandemic means that EUIs must continually adapt their processes. The report aims to support them in what appears to be a long-lasting challenge, which will likely continue to have an impact even after the end of the pandemic.





The survey results will feed into updating existing EDPS guidelines, or contribute to the development of new guidelines, depending on the evolution of the pandemic and the new practices that will continue once it is over. The survey results will also inform the EDPS' execution of audits and investigations under [Article 58](#) of Regulation (EU) 2018/1725.

The report was presented to the EUIs' data protection officers at the network of DPO meeting in December 2021, and was made public, on the [EDPS website](#), in early 2022.

### 3.2.3.

## The use of ICT tools, remote working tools and social media by EUIs

On 17 March 2021, colleagues from the EDPS' S&E Unit carried out a training session at the European School of Administration, focusing on the data protection implications of information and communications technology (ICT) tools, remote working tools and social media used by EUIs.

Based on, but not limited to, the [EDPS' Orientations](#) published in July 2020, S&E colleagues reiterated that:

- EUIs' staff should follow their EUIs' established protocol(s) and involve their data protection officer(s) and IT department(s) when selecting ICT tools;
- EUIs should carefully assess the security, confidentiality and privacy features of the proposed tools and evaluate their potential risks for individuals' personal data, also taking into account any privacy-friendly alternatives that may be available;
- the terms of contracts with ICT providers should reinforce EUIs' control over who processes individuals' personal data and how it is processed; technical and organisational measures must also be put in place.

The training session also emphasised that the use of social media and videoconference tools should be considered like any other ICT tools when

assessing their data protection implications and adopting necessary measures to ensure that individuals' privacy is protected. We felt it was necessary to provide training on social media due to the increase in the use of these tools by EUIs during COVID-19 to connect with their audience.

The EDPS intends to test privacy-friendly and open-source alternatives to major social media and videoconferencing tools in the upcoming future.

### 3.3.

## EDPS Cooperation with EUIs' data protection officers

One of the EDPS' key roles is to supervise the compliance of EUIs with Regulation (EU) 2018/1725. Amongst other actions taken, one of the ways we ensure that EUIs are consistently complying with data protection law is by advising, guiding and collaborating with their respective Data Protection Officers. The DPO is a crucial interlocutor and key contact point between the EDPS and their EUI.

### 3.3.1.

## Meeting with the network of DPOs

Due to the important role played by DPOs between the EDPS and EUIs, a meeting is held twice a year to discuss current and upcoming data protection challenges in the year. This provides an opportunity to discuss priorities of the DPOs of EUIs and to identify areas where extra guidance or support from the EDPS is needed.

For the first time, a group of DPOs, the DPO Support Group, actively contributed to the organisation of both EDPS - DPO Meetings in 2021. The DPO Support Group's commitment and hard work contributed to making both meetings a success.

### 1. DPO meeting in June 2021

The 4 June 2021 marked [the 49th meeting](#) of the EDPS and the European institutions, bodies and agencies' network of Data Protection Officers (DPO).



A series of online workshops and exchanges were held on current data protection issues, from data protection breaches to the use of software alternatives to large-scale providers, as well as international transfers and cloud services, to name a few examples.

The first workshop focussed on the [EDPS Guidelines on personal data breach notifications](#). The second workshop was dedicated to the use of software alternatives to large-scale providers. International transfers and cloud services were the central issues discussed during the third workshop.

EDPS colleagues and the EUIs' DPOs shared their experiences of looking for possible and pragmatic solutions to the challenges faced by all EUIs in this area.

## 2. DPO meeting in December 2021

On what should have been the [50th EDPS-DPO meeting](#) with the DPO of the EUIs, the EDPS held a second 49th EDPS-DPO meeting online, on 14 December 2021, due to the ongoing COVID-19 pandemic.


The EDPS started the meeting with an overview of the most recent and important developments and achievements of the EDPS and the EDPB.

This was followed by a brief presentation on the results of the EDPS survey on the EUIs' data processing operations in connection with COVID-19, launched in 2020. The meeting continued with two workshops, one on manual contact tracing and another on access control, both organised with the valuable help of the DPO Support Group.

During the workshop on manual contact tracing, the EDPS considered challenges resulting from enforcing data retention periods, and the interplay between contact tracing within an EUI and national health authorities.

During the access control workshop, the data protection risks of verifying COVID-19 certificates digitally, or using QR-scanning applications for example, were examined.

During both workshops, the EDPS reviewed the EDPS' guidance on COVID-19 matters and EUI's current practices.



The meeting led to productive discussions on how to protect individuals' personal data in times of COVID-19. This productive and successful meeting would not have been possible without the active participation of the EDPS' S&E Unit, the EDPS' Technology & Privacy Unit, the DPO support group, and of course all of the EUIs' DPOs.

With these online workshops, the EDPS aimed to recreate in 2021 the interactive and dynamic environment akin to its traditional in-person meetings pre-COVID-19. It was also an opportunity for DPOs to share their concerns, queries and reflections with the EDPS about how to put data protection rules into practice in their day-to-day work when the processing of individuals' personal data is involved.

These meetings are one of the ways to reinforce trust, improve communication and foster a close cooperation between the EDPS and the network of DPOs in order to be able to face many upcoming challenges in data protection efficiently and collectively.


### 3.3.2.

## Welcoming new data protection officers

The EDPS' S&E colleagues offer one-to-one data protection training sessions to newly-appointed DPOs and assistant DPOs.

These personalised training sessions started in 2020. This is a voluntary and informal training delivered in English by the S&E unit. This style of training allows for a more personalised and tailor-made session. In addition, it allows both the DPOs and S&E colleagues to delve into deeper topics and issues relating to data protection. These training sessions also offer an opportunity for DPOs to enhance their knowledge on a variety of different training sessions associated with data protection.

Topics covered during these sessions are based on the DPOs' and Assistant DPOs' needs and requirements. As such, this may include a refresher of the basics, such as an overview of the data protection principles, or a training session that is more geared towards the tasks of the EU institution they have been appointed to.



These sessions are one of the ways for the EDPS to foster good collaboration and collegiality with its DPOs. Despite these training sessions being held remotely, the eagerness for them has continued.

### 3.3.3.

## Quick News for DPOs

In 2021, we continued to publish its “Quick News for DPOs” editions, a monthly newsletter for data protection officers of EUIs.

The DPO newsletter was created in 2019 as the EDPS recognises the importance of staying in touch regularly with data protection officers to foster good communication and collaboration, especially during the COVID-19 pandemic.

The newsletter provides DPOs with the latest updates on EDPS Guidelines, Recommendations, Opinions, and more, that are directly relevant to their day-to-day work, their institution’s core business and current data protection developments that concern them or their institution.

While preserving the anonymity of the institution, body or agency in question, we also share information about common questions, complaints or consultations received from an EUI, as these can help DPOs know what measures to put in place if they encounter the same or a similar situation.

Ten editions of the DPOs Quick News were published in 2021. Some of the topics covered throughout the year include:

- basic data protection principles;
- transfers of personal data to non-EU/EEA countries;
- protecting individuals’ data in the context of recruitment;
- how to handle employees’ data in the context of a pandemic.

The newsletter is also used to promote upcoming training sessions or events organised by the EDPS for DPOs and other members of staff of EUIs, which DPOs are always encouraged to join. Each edition also includes a data protection recommendation of the month.

### 3.3.4.

## EDPS-DPOs roundtable

In order to foster cooperation and communication between the EDPS, as a data protection authority, and the EUIs' DPOs, four EDPS-DPOs roundtables were organised in 2021. Colleagues from the Supervision & Enforcement and from Technology & Privacy Units of the EDPS, together with the EDPS' DPO, participated in these meetings.

The first meeting focused on the EDPS-DPOs cooperation, while the following meetings were on topical issues, such as transfers of personal data outside of EU/EEA, the use of video - conference tools and processing activities related to COVID-19.

### 3.3.5.

## Data protection training for EUIs' staff

In addition to providing support to EUIs' data protection officers, we also deliver general and specialised training sessions to staff members of the EUIs. These training sessions are often organised at the request of the DPO of a particular institution on behalf of its members of staff, and are specifically tailored to staff's day-to-day tasks that have an impact on data protection and that involve the processing of personal data.

In 2021, we gave 25 trainings to a number of EUIs mainly in the field of public procurement, outsourcing of data processing, personal data breach notifications and transfers of personal data.

In 2021, we launched an online course titled: "EUDPR fast-track training course for practical application in your daily task", which was made accessible to all EUIs' members of staff via the online platform, EU Learn.

The course provides EUIs' members staff with an overview of Regulation 2018/1725 by explaining key concepts and their obligations under this Regulation, as well as giving them practical advice on how to ensure that individuals' personal data that they process is protected.

The course is divided into 5 comprehensive modules; the first four modules cover the basics as well as more complex notions, such as:

- the accountability principle;
- data protection by design and by default in practice;
- data protection impact assessments;
- what to do when transfers of personal data with other EUIs or entities outside the EU/EEA occur.

The fifth and final module gives EUIs' staff the opportunity to assess themselves with 38 questions on data protection. Detailed feedback and more information for each question is also available to enhance their learning experience.

Whether EUIs are handling selection and recruitment procedures, staff appraisals, administrative inquiries, organising events, dealing with contracts, grants and tenders: personal data is everywhere. Members of staff have obligations and rights under Regulation (EU) 2018/1725, which they must be aware of; these are summed up in this course.

### 3.4.

## Addressing complaints from individuals

Under Regulation (EU) 2018/1725, individuals have the right to lodge a complaint with the EDPS if they consider that the processing of their personal data infringes the Regulation. Staff members of the EUIs can submit complaints without being personally affected by the alleged infringement of the Regulation.


In 2021, we received more than 320 complaints, out of which 50 were admissible; 3 complaint inquiries resulted in the EDPS using its [corrective powers](#).

### 3.4.1.

## Disclosing candidates' results in EU competitions

We have received several complaints related to the processing of personal data of candidates participating in EUIs' recruitment procedures.

In July 2021, we addressed complaints against two different EUIs, in



which both complainants submitted that they were not granted access to their respective assessment results following their participation in an EPSO competition as part of the recruitment procedure.

We reiterated that it is crucial that the EUI which organised the competition preserves the secrecy and independence of the panel assessing candidates. At the same time, the EUI should have ensured that individuals participating in these competitions have access to their results. To achieve this, the EUI in question should provide candidates with their assessment results in a clear and intelligible form without disclosing the identities and comments of the members of the selection panel.

Following these two complaints, both candidates received appropriate and transparent feedback on their performance during these competitions.

Our advice allows EUIs involved in the organisation of competitions to respect the privacy of interested individuals on one hand, and to offer transparent and comprehensive information to candidates being assessed in these competitions on the other.

### 3.4.2.

## Unauthorised access to employee's data

In July 2021, we received a complaint of an EU institution's employee claiming that the institution's leave coordinators had unauthorised access to their personal information regarding special leave.

Employees of EUIs may request special leave on personal grounds, for example in the event of a serious illness that themselves or their immediate family may have which prevents them from working. Reasons determining special leave may include sensitive information. Access to this information can only be given to the direct manager of the staff member involved.

Following the complainant's claim, in which they submitted that the EUI's leave coordinators had access to sensitive information on their mother's and their child's illnesses, we carried out an investigation.

With this investigation, the EUI in question reviewed and corrected their policy to ensure that the personal data of employees that are collected are

limited to what is necessary and relevant to a specific purpose. Likewise, access to employees' personal data should be limited to members of staff that need such data to perform their task, such as determining the grounds for special leave of an employee.

By amending their policy, the EUI in question focused on protecting individuals' personal data and avoided unnecessary intrusion into their employees' rights and privacy.

We also confirmed that it is the responsibility of the EUI's [data controller](#) to analyse the risks their decision(s) may have on their employees' privacy rights.

### 3.4.3.

## Statistics of the complaints received

In 2021, we received 327 complaints, showing an increase of 33%, compared to 2020. Out of these, 277 were inadmissible, the majority relating to data processing by national authorities or private entities as opposed to the processing of data by an EUI. We replied to all inadmissible complaints, directing the complainant to the relevant authority. The remaining 50 complaints required in-depth inquiry. In 2021, the EDPS issued 28 decisions on admissible complaints. We received 50 admissible complaints in 2021, in comparison to receiving 43 admissible complaints in 2020.

Year	Complaints received	Admissible	Inadmissible
2021	327	50	277



EU Institution, office, body or agency	Number of complaints
European Commission (EC)	12
European Anti-Fraud Office (OLAF)	4
Council of the EU (Council)	3
European External Action Service (EEAS)	3
European Investment Bank (EIB)	3
European Personnel Selection Office (EPSO)	3
European Union Agency for Law Enforcement Cooperation (EUROPOL)	5
European Parliament (EP)	2
European Union Agency for Law Enforcement Training (CEPOL)	1
European Court of Auditors (ECA)	1
European Court of Justice (ECJ)	1
European Data Protection Supervisor (EDPS)	1



European Insurance and Occupational Pensions Authority (EIOPA)	1
European Union Agency for Cybersecurity (ENISA)	1
EP - Member of the EP	1
European Public Prosecutor's Office (EPPO)	1
European Research Council Executive Agency (ERCEA)	1
European Securities and Markets Authority (ESMA)	1
European Union Intellectual Property Office (EUIPO)	1
European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)	1
European Border and Coast Guard Agency (FRONTEX)	1
Single Resolution Board (SRB)	1
Community Plant Variety Office (CPVO)	1
<b>Grand total</b>	<b>50</b>

Use of corrective powers	
<p>Article 58(2)(a)</p> <p>(To issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation)</p>	1
<p>Article 58(2)(b)</p> <p>(To issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation)</p>	2

### Number of complaints received

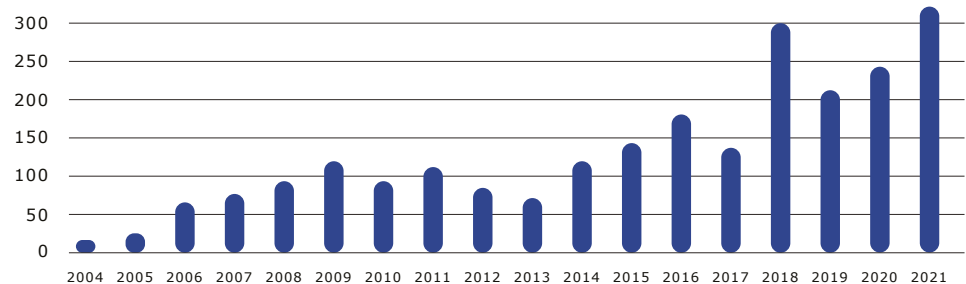



Figure 2: Statistics of complaints received

### 3.5.

## Data Protection audits

As part of its supervisory work, the EDPS regularly conducts audits to verify how data protection is applied in practice by EUIs. During an audit, the EDPS can verify compliance and make recommendations, if areas for improvement are identified.




Audits are carried out according to the Annual Inspection Plan. To establish this plan, we conduct a risk analysis and consider the resources available to carry out audits. Although, we reserve the right to carry out audits on a random basis, we consider various factors when deciding which EUI to audit, including the categories of data the EUI processes (e.g., health data are particularly sensitive) and the compliance of the EUI with previous EDPS decisions.

The three stages of an audit include:

1. **Pre-audit** – The EUI and its DPO are usually informed at least four weeks in advance and sometimes asked to provide information and documents prior to an audit.
2. **During an audit** –The EDPS meets the EUI’s staff members who are responsible for the processing of personal data, requesting information and demonstrations of how the EUI processes individuals’ personal data in its day-to-day work. The results of these meetings are collected, recorded, and submitted to the audited EUI to correct any factual errors.
3. **Post-audit** –The EDPS will provide appropriate feedback to the EUI concerned in an audit report. This contains a roadmap of recommendations to put in place where necessary.

Staff of the EUI that is audited (and its DPO, if they decide to do so) are actively involved in the process, for example through interviews or on-the-spot demonstrations. EDPS auditors are subject to strict confidentiality obligations. All EUIs’ staff members are obliged to assist EDPS auditors upon request under [Article 32](#) of Regulation (EU) 2018/1725. This could include the provision of information on the data processing activities the EUI carries out in its day-to-day work or granting access to personal data and granting access to the premises.

With COVID-19 preventing us from conducting fieldwork, we adapted our audit planning and moved to remote audits in 2020. Such adapted procedures allow us to continue our supervisory work, by reaching out to a high number of EUIs, their data protection officers, and EUI staff processing individuals’ personal data in their day-to-day work.



In 2021, we conducted a remote audit of Internal Rules established by EUIs under [Article 25 of Regulation 2018/1725](#), which, under certain circumstances, allows for the restriction of individuals' data protection rights.

Remote audits are likely to continue post-COVID-19 in a selection of circumstances. In one of our first audits, which included fieldwork during the pandemic in October 2021, we verified whether retention periods stipulated for COVID-specific measures had actually been put in place. Other audits that were conducted on the spot include Europol and Eurojust.

### 3.5.1.


## EDPS audit on newsletter subscriptions

In April 2021, we published the outcome of the [remote audit](#) on how EUIs inform individuals about the way their personal data is processed when signing up to newsletters and other similar subscriptions.

With the absence of in-person events and other outreach activities due to COVID-19, EUIs have increased their online presence. The sending of newsletters is an effective way of reaching out to individuals and stakeholders. EUIs should lead by example in providing transparent information to individuals on the way their personal data is being handled.

We found that most EUIs comply with the information and transparency requirements set out in Regulation 2018/1725. Even before receiving the EDPS' recommendations following the audit, the majority of EUIs proactively took interim measures. After announcing the audit, EUIs revised for example their data protection statements or improved the accessibility of information. These measures aim to ensure that individuals have easy access to clear information on the EUIs' websites about how their personal data is processed when subscribing to newsletters.

This [audit](#), for which no on-the-spot action was required, has been part of a number of audits conducted remotely by the EDPS due to the COVID-19 crisis.



### 3.5.2.

## EDPS audit on an individual's data right restrictions

We carried out a remote audit to EUIs in order to verify the compliance with [EDPS Guidance on Article 25 of Regulation \(EU\) 2018/1725](#), published in June 2021.

[Article 25](#) of Regulation (EU) 2018/1725 states that EUIs' Internal Rules may restrict the application of individuals' data protection rights, under the condition that such restrictions respect the essence of the fundamental rights and freedoms affected, and is a necessary and proportionate measure in a democratic society to safeguard a certain number of legally protected interests.

As such, the EDPS audit aimed at understanding how EUIs have taken into account the recommendations issued by the EDPS when drafting their Internal Rules. We looked further into the application of these Internal Rules in practice by examining actual cases of EUIs restricting individuals' data protection rights.

The decision to carry out a remote audit on these topics was influenced by the importance of the practical implementation of Article 25 on restrictions of individuals' data protection rights. The fact that Internal Rules restrict such rights may eventually interfere with the fundamental right to personal data protection, and therefore could negatively impact and diminish its scope of protection for individuals.

### 3.5.3.

## EDPS audit on data retention periods.

As a follow-up to the input provided by EUIs in the context of the COVID-19 Survey, the EDPS decided to audit two big Brussels-based EUIs that have specific processing operations in place due to COVID-19, and for which data retention periods had already run out mid-2021.

Data retention refers to all obligations on the part of controllers to retain personal data for certain purposes; to limit how long personal data is retained is part of data minimisation.

The rule of thumb is “as long as necessary, as short as possible”, although sometimes legal requirements may impose otherwise.

Although the audit’s scope was limited, conducting the audit intended to send out a strong message to all EUIs that COVID-related processing operations must be temporary.

Other reasons that motivated the EDPS to carry out an audit include:

- the potentially high number of individuals concerned by COVID-specific processing operations;
- the considerable impact on individuals given the sensitive nature of the personal data processed;
- the learning outcomes of this audit for EUIs, but also other public bodies within the EU Member States.

### 3.6.

## EDPS investigations

Under [Article 58\(1\)](#) of Regulation (EU) 2018/1725, the EDPS has the power to carry out investigations. These investigations start on the basis of information received from third parties, for example complaints, press reports, or carried out on the EDPS’ own initiative.

Our investigative powers allow us, in particular, to order controllers and processors to provide information required for its tasks, and to obtain access to all personal data and to any premises of the controller and the processor. The latter includes any data processing equipment and means of processing.

### 3.6.1.

## Investigations following the “Schrems II” judgment

In October 2020, we issued a [strategic document](#) aiming to monitor the compliance of EUIs with the “[Schrems II](#)” judgment in relation to transfers of personal data to non-EU/EEA countries, and in particular to

the United States (US), to ensure that ongoing and future international transfers are carried out in accordance with EU data protection law. We developed an action plan to streamline compliance and enforcement measures, *distinguishing* between short-term and medium-term compliance actions.

Our strategy builds on the cooperation and accountability of controllers to assess, in line with the Court's ruling, whether the *essentially equivalent standard of protection* is guaranteed when personal data is transferred to (or remotely accessed by) recipients in non-EU/EEA countries.


As a first step, we ordered EUIs to report on certain categories of transfers of personal data to non-EU countries. Two priorities should be addressed in the short-term: ongoing controller to processor contracts and/or processor to sub-processor contracts involving transfers of data to non-EU/EEA countries.

The analysis of the information reported to the EDPS confirmed that EUIs increasingly rely on cloud-based software and cloud infrastructure or platform services from large ICT providers, of which some are based in the US and are therefore subject to legislation that, according to the "Schrems II" Judgment, allows disproportionate surveillance activities by the US authorities.

As part of the strategy, we launched two investigations in May 2021, which are to be continued in 2022, regarding:

- the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EUIs;
- the use of Microsoft Office 365 by the European Commission.

The objective of the first investigation is to assess EUIs' compliance with the "Schrems II" judgment 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 US.



We underlined that, although the “Cloud II contracts” were signed in early 2020 before the “Schrems II” judgement and that both Amazon and Microsoft have announced new measures with the aim to align themselves with the judgement, these announced measures may not be sufficient to ensure full compliance with EU data protection law.

The aim of the second investigation into the use of Microsoft Office 365 is to verify the European Commission’s compliance with the [Recommendations](#) previously issued by us in 2020 on the use of Microsoft’s products and services by EUIs. This also includes compliance regarding international transfers.

With these investigations, the EDPS aims to help EUIs improve their data protection compliance when negotiating contracts with their service provider.

We believe that EUIs are well positioned to lead by example when it comes to privacy and data protection. The announced steps are part of a continuous cooperation between the EDPS and the EUIs to ensure a high level of protection of these fundamental data rights.

### 3.7.

## The EDPS’ advisory powers

### 3.7.1.


## Own-Initiative Opinions

As the data protection authority of EUIs, we have the power to issue Opinions on any matter related to the protection of personal data according to [Article 58\(3\)\(c\)](#) of Regulation (EU) 2018/1725. In line with its commitment to take the long-term view of trends in data protection and in the legal, societal and technological context, we issue Opinions on a wide range of EU-level policy initiatives with the aim to provide decision-makers with timely insight and advice.

### 1. The processing of biometric data

In March 2021, the EDPS published an own-initiative [Opinion](#) on a proposed computerised system (Proposal) to register the attendance





of Members of the European Parliament's (MEPs) to Plenary sessions. Amongst other reasons, registering MEPs attendance is necessary to document which MEPs are eligible for an allowance under the [internal rules governing the status of MEPs](#).

Under the Proposal, the current paper-based signing system would be replaced with a solution based on an optical fingerprint scanner. For each Plenary session, MEPs would need to place their fingers on a local fingerprint reader which would scan the fingerprints to extract the necessary information and compare it to a previously recorded template of the fingerprints.

This proposed system touches on sensitive data protection topics, such as the use of biometric data – in this case fingerprints – which allows the unique identification of individuals; and automated decision-making – in this case the processing of individuals' fingerprint data without human intervention.


We focused on whether the system would be truly necessary and proportional to the objectives set out in the proposal – in particular to avoid fraudulent sign-ins. At the same time, it should also be considered whether this type of data and its processing can be justified under Regulation 2018/1725; and whether the European Parliament (EP) can rely on an exception under the Regulation which prohibits the processing of this type of data. [Data controllers](#) need to be able to demonstrate that such exception applies.

Before putting in place similar systems, data controllers should conduct a [data protection impact assessment \(DPIA\)](#) examining alternatives to the proposed system that do not require the same amount of sensitive data. When comparing the different alternatives, the controller should evaluate the impact and risks that each option may have on individuals' personal data. In the case at stake, the EP conducted a DPIA, but we believe that the EP should explore less intrusive alternatives in terms of data protection.

### 3.7.2.

## EDPS Consultations

EUIs may consult the EDPS for guidance on their planned processing



operations and on their compliance with data protection law. Depending on the complexity of the EUI's request, we provide advice in different forms, via calls to the DPO hotline, informal advice to staff and formal signed letters, for example. Whilst we provide guidance, the responsibility for ensuring compliance with data protection law remains with the EUIs.

EUIs may also be obliged to consult us on planned processing operations, particularly when they intend to adopt internal rules restricting individuals' right to data protection and when extra-EU transfers of personal data require prior authorisation. When replying to such requests, we provide input on any necessary improvements to be made.

In 2021, we replied to 71 consultations: 54 of these consultations were related to supervision and enforcement matters, and 17 of these consultations were on matters related to the Area of Freedom, Justice and Security ([see chapter 4](#)). These include:

- informal exchanges at staff level;
- Opinions under [Article 41](#) of Regulation (EU) 2018/1725, which involves administrative measures and internal rules relating to an EUI's processing of personal data;
- Opinions under [Article 57\(1\)\(g\)](#) of Regulation (EU) 2018/1725, when the EDPS advises an EUI either on its own initiative or upon request;
- Opinions under [Article 58\(3\)\(c\)](#) of Regulation (EU) 2018/1725, when the EDPS advises an EUI on its own initiative; and
- Opinions under the specific Regulations on [Europol](#), [Eurojust](#) and [EPPO](#).

In addition, we issued two Opinions following prior consultations of EUIs under [Article 40](#) of the Regulation before the start of their processing operations.

Most of the consultations we received in 2021 were on health matters, such as COVID-19 issues, transfers of personal data to non-EU/EEA countries, and ethical matters.

### 1. COVID-19 and other health matters

Within the scope of consultations on COVID-19 and other health matters, the EDPS is consulted by the EUIs on the impact of the pandemic on

individuals' personal data, as well as on ways in which EUIs should adapt their working environments to mitigate such impact.

#### 1A. Verifying Digital Covid Certificates prior to entering EUIs' premises

In October 2021, we issued an [Opinion](#) on the use of mobile applications to verify Digital COVID Certificates before visitors can enter the European Commission's premises in Brussels and Luxembourg.

We recommended that individuals wishing to enter the EUIs' premises are clearly informed about how their data will be processed and for what purposes. This should be communicated to individuals via several methods, or communicated to them prior to their entrance into the building.

We also suggested that a verification procedure is planned to prevent any individual from entering the EUIs' premises without having had their Digital COVID Certificate checked.

It is also recommended that EUIs check whether the mobile applications that may be used to verify Digital COVID Certificates comply with the data protection law, Regulation (EU) 2018/1725, and other data protection principles to protect individuals' personal data.

#### 1B. Verification of Digital COVID certificates for visitors and staff

The EDPS was [consulted](#) by the Joint Research Centre (JRC) of the European Commission regarding the mandatory verification of Digital COVID Certificates for staff and visitors at its Ispra site in Italy, after an Italian decree obliged employers to check employees' COVID certificates.

Taking into account that the Site Agreement between the European Commission and Italy provides that national health and safety rules apply to the JRC site, the EDPS recommended that the JRC:

- follows any national health guidance on using the COVID certificate passes in the context of employment;
- informs individuals concerned of the conditions on entering the premises;

- makes sure that measures related to COVID-19 are periodically assessed and re-evaluated in light of the evolving COVID-19 crisis.

The consultations described above are just a few examples to illustrate the EDPS' work in this area. As the COVID-19 pandemic evolved, so did its work, advice and recommendations to EUIs. To this end, the EDPS advised EUIs to periodically assess the procedures taken to verify individuals' Digital COVID Certificates, as well as assess alternative organisational and sanitary measures to limit the spread of COVID-19.

### 1C. The manual contact tracing of COVID-19 cases

For the purpose of protecting health and to minimise the risk of spreading COVID-19 at the workplace, an EUI may process personal data concerning confirmed and suspected COVID-19 infections of the staff members and members of their household.

We issued an [Opinion](#) on the legal basis, under Regulation (EU) 2018/1725, which allows the processing of personal data for the purposes of manual contact tracing on 26 February 2021.

Taking into account the employment context of such contact tracing system, it is unlikely that consent is freely given, thus the majority of cases will not be considered as a valid legal ground for the processing operation.

Indicatively, lawful grounds could be the necessity of the controller's obligation to process personal data in the field of employment, social security and social protection law or for the assessment of the working capacity of the employee.

Therefore, an EUI can set up manual contact tracing of COVID-19 cases provided that the lawfulness, when processing special categories of data, (i.e., health data) is respected, the conditions for a safe work environment and the conditions for the management of medical leave are met. This means that the control and supervision over the processing of sensitive data about health should remain with the medical professionals bound by a duty of medical confidentiality.

## 1D. Remote invigilation of recruitment procedures

Adapting to the outbreak of COVID-19, some EUIs have carried out certain of their recruitment and selection procedures - including written and practical tests - remotely.

In light of this, an EUI consulted us on the possibility of having an external contractor, based in the EU, invigilating the remote exams that are part of the EUI's selection and recruitment procedure. Such process may involve the external invigilator to process personal data, such as asking candidates passing tests for their ID.

We summarised the recommendations to the EUI in an [Opinion](#) published in October 2021. In this Opinion, we advised the EUI:


- to identify the risks for candidates' personal data and to plan any measures to mitigate such risks;
- to monitor the evolution of the COVID-19 pandemic and to assess whether it is necessary or not to remotely invigilate written tests, or any other aspects of the EUI's selection procedure;
- to make sure that the processing envisaged is necessary, lawful and justified, according to the conditions laid down in [Article 5](#) of Regulation (EU) 2018/1725 for the task(s) at hand.

In addition, we recommended that the EUI assesses how likely it is for special categories of personal data - data concerning health, data revealing racial or ethnic origin for example - to be disclosed during the invigilating phase of the recruitment procedure. Not only should the level of such risk be determined and that the EUI in question should plan mitigating measures to protect candidates, but the processing of special categories of data should also be justified, lawful and necessary for the task(s) at hand, according to the rules about the processing of sensitive personal data.

The EUI was given three months to provide an updated DPIA before any processing of individuals' personal data occurs. The DPIA process aims to provide assurance that the EUI adequately addresses the privacy and data protection risks of 'risky' processing operations, in a structured way.

## 1E. ECDC's use of data related to COVID

The European Centre for Disease Prevention and Control (ECDC)



[consulted](#) the EDPS regarding the processing of data available on the GISAID platform.

The GISAID platform is the most important entity worldwide that provides access to genomic data on influenza and corona viruses. This platform is supported by a non-profit organisation and provides a publicly accessible database designed by scientists for scientists to improve the sharing of information about influenza virus and coronavirus. This database includes not only genetic sequence, but also related clinical and epidemiological data that is encoded by relevant authorities of the EU Member States and by scientists. This is a curated database, which means that a GISAID team reviews each record submitted by the users before making the data available. The GISAID team also attributes an identifier to trace back the data. EU Member States insert data under a national identifier and then the GISAID Team replaces that identifier with another.

The ECDC requested access to the data regarding corona viruses processed in this platform for epidemiological surveillance purposes.

In our consultation, we considered that the data processed in the database was personal data, in spite of the code attributed by the GISAID Curation Team. To make our decision, we took into account a number of factors, including the special relationship between the ECDC and the EU Member States and the data at stake: health data and genetic data. We concluded that even though the data is pseudonymised, it could not be excluded that individuals' data may be indirectly identifiable.

Examining the circumstances, we determined that the ECDC would be acting as a controller if it was processing personal data because the ECDC determines the purpose of the processing when it extracts specific categories of data from the GISAID platform, using its own means, in order to accomplish its own tasks. Therefore, the ECDC and GISAID are separate controllers.

To ensure that the ECDC processes individuals' health data in compliance with the EU's data protection laws, we provided guidance on:

- data retention periods;
- the need to inform their staff about not taking actions to obtain additional information which would re-identify individuals from their data;

- asking the ECDC to regularly check the level of security of this processing operation.

## 2. Transfers of personal data to non-EU/EEA countries


### 2A. Subscribers' consent to transfers of personal data

We were consulted in November 2020 by an EUI on transfers of personal data to a non-EU/EEA country resulting from the use of a newsletter service of this EUI. Interested parties could subscribe to the newsletter via this EUI's website "*based on consent*" and "*after being provided with very clear information (also on the risks related to the transfers)*". The service provider was based in the EU but had sub-processors in the US.

In our Opinion, issued in July 2021, we highlighted that the EUI needed to ensure the lawfulness of the processing operation according to [Article 5\(1\)](#) of Regulation (EU) 2018/1725. More specifically, for standard outreach activities, such as the publication of newsletters, the EUI needed to ensure that individuals give their valid consent. Such consent must be freely given by a clear affirmative act and it must be specific, informed and unambiguous, according to [Article 3\(15\)](#) of Regulation (EU) 2018/1725.

Thus, it is important that the EUI primarily assesses, together with the data processor, the availability of any newsletter-publishing solutions not involving the transfer of personal data to the US. The EUI must only use a processor that will guarantee the use of appropriate technical and organisational measures, so as to comply with Regulation (EU) 2018/1725.

If the data processing involves the transfer of personal data, we underlined that the EUI needs to comply with the additional requirements laid down in [Chapter V](#) of Regulation (EU) 2018/1725 (including Article 50(1)(a) where relevant). From a practical standpoint this means that, prior to the transfer - before newsletter subscribers provide their personal data, the EUI needs to ensure that subscribers receive specific information about the transfer of their personal data, including its risks, to a US-based sub-processor with a view to subscribing to the newsletter. In addition, the EUI needs to ensure that participants explicitly consent to the transfer of their data to the US-based sub-processor with a view to



subscribing to the EUI's newsletter, in addition to their consent on the processing operation in general.

### 3. Ethical matters

#### 3A. Internal rules restricting individuals' data rights

Data protection law grants certain rights to individuals, including rights to erasure, information rectification and right to access. Whilst these rights should be strictly respected, EU law also provides that they can be restricted in certain specific circumstances, with the safeguards laid down in Regulation (EU) 2018/1725.

EUIs may restrict individuals' right to data protection on the basis of their internal rules. Such restrictions are only possible in matters relating to the operation of the EUI in question, and where each restriction is linked to an applicable legal ground. EUIs are required to consult the EDPS when drawing up such internal rules through a process, which acts as an additional control to ensure compliance with the Regulation.

In 2021, the EDPS issued 10 Opinions on draft Internal Rules, and on restrictions to individuals' right to data protection. Most of these Opinions can be found on the EDPS website [here](#).


#### 3B. Status of confidential counsellors

An EUI raised a question on whether confidential counsellors and other staff members may be considered as 'processors' when they process personal data in the context of informal anti-harassment procedures, or whether they should be, in all circumstances, considered as 'individuals acting under the authority of the controller', under Regulation (EU) 2018/1725.

In our [Opinion](#), published in July 2021, we recommended that confidential counsellors, in so far as they are staff members of an EUI, are considered as individuals acting under the authority of the controller in line with [Article 30](#) of Regulation (EU) 2018/1725.

We stressed that while the function of a confidential counsellor has particular characteristics, including a strict duty of confidentiality regarding the controller, it is nonetheless essentially comparable to certain other functions that staff members may exercise. On the one





hand, they cannot receive any specific instructions from the controller while acting as confidential counsellors; while on the other hand, they must process personal data according to instructions provided by the EUI by the means of internal rules or anti-harassment procedures.

We added that, in order for a staff member to be considered as a person acting under the authority of the controller, it is not necessary that the controller gives counsellors specific instructions, as long as general instructions amount to a sufficient basis for any relevant processing of personal data are provided by the controller.

### 3C. Trade Unions' unsolicited communication

In April 2021, we published an [Opinion](#) following an EUI's request for recommendations to ensure that the EUI's staff are able to unsubscribe from unsolicited e-mails from trade unions and staff associations.

Such email communication is based on a Framework Agreement signed between the EUI and the unions in 2008. The Framework Agreement governs the relations between the EUI and the trade unions. It confirms that EUI officials may be members of a trade union, and so can their retired officials and other servants. Trade unions are authorised to send e-mails from their functional mailbox to the EUI's staff, subject to the good practices set out in a code drafted specifically for that purpose.

Based on this Agreement, trade unions were sending e-mails, both to their members and to non-members without any previous subscription, some of which could be considered as "promotional emails and an indirect way to gain more supporters/members".

We pointed out to [Article 38\(2\)](#) of Regulation (EU) 2018/1725, which obliges EUIs to take all the necessary measures to prevent personal data contained in directories from being used for direct marketing purposes.

The fact that unions were sending marketing e-mails demonstrated a failure to comply with the Regulation.

Amongst other recommendations, we advised that the EUI clearly set out that its authorisation does not cover direct marketing and that the code should provide that trade unions must offer clear options to the recipients of these emails on how to unsubscribe from trade union's mailing lists.

### 3D. Individuals' access to personal data during an investigation

In December 2021, we were consulted by an EUI on whether they need to inform an individual that some of their personal data had been transmitted to [OLAF](#), the European Anti-Fraud Office, in the context of an investigation, according to [Article 3\(13\)](#) of Regulation (EU) 2018/1725.

Subject to specific circumstances and conditions, Regulation (EU) 2018/1725 provides other legal grounds that EUIs can rely on to not provide information to an individual whose actions and behaviour are investigated or to an individual who is related to an investigation. The EUI in question was therefore wondering if relying on the specific nature of OLAF as a 'non-recipient' under Article 3(13) would suffice to justify not providing information to the individual who is being investigated or who is related to an investigation.

Weighing up the EU data protection law and circumstances presented to us, we concluded that EUIs could not just rely on Article 3(13). EUIs had to, in addition to these special circumstances, rely on another legal ground, specified in the Regulation, such as an exception or a restriction, to justify not giving information to an individual concerning an investigation related to them or about them.

#### 3.8.

## Cooperation with the EFTA Surveillance Authority

The [EFTA Surveillance Authority \(ESA\)](#) is responsible for ensuring that Iceland, Norway and Lichtenstein respect their obligations under the [European Economic Area \(EEA\) Agreement](#).

In 2021, the EDPS provided staff-level guidance on the physical move of the ESA to its new and shared premises, to be known as the 'EFTA House'. ESA shares its building with the European Free Trade Association (EFTA) and the Financial Mechanism Office (FMO), bringing all three EFTA Brussels-based organisations into one building.

While these three authorities are of course closely related, having shared facilities raises several questions regarding the processing of personal


data of their respective staff and operations. ESA has started to address these questions through its temporary agreement on data protection, signed with the EFTA and the FMO.

Building on this agreement, ESA itself should now continue to ensure compliance with its own data protection framework, which closely aligns with the one applicable to EUIs, Regulation (EU) 2018/1725.



## CHAPTER FOUR

# The Supervision of the Area of Freedom, Security and Justice



As part of its work, the EDPS also supervises the data processing operations of the following bodies and agencies:

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

These bodies and agencies are part of the Area of Freedom Security and Justice (AFSJ). According to [Title V of the Treaty on the Functioning of the European Union](#), the 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. The AFSJ also includes asylum and immigration policies, police cooperation and the fight against crime, such as terrorism; organised crime; trafficking of human beings; drugs.

#### 4.1.

### A holistic approach to the supervision of AFSJ bodies and agencies

The EDPS highlighted in its [Strategy for 2020-2024](#) the challenges that the patchwork of measures in the areas of police and judicial cooperation and border management was creating for its supervisory and enforcement powers. In order to address these challenges, the EDPS committed to identifying discrepancies in the standards of data protection within EU law in the AFSJ, and to enforce the rules consistently as a way to actively promote justice and the rule of law, as well as a vision of digitalisation that enables us to value and respect all individuals.

The EDPS also observed that successive legislative reforms are fostering AFSJ agencies and bodies to increase their cooperation and consequently their exchange of personal data. These exchanges are likely to increase in the coming years, as the interoperability framework and the hit/no hit

access between agencies become operational. The hit / no hit concept gives effect to respective regulations where one agency can make a query into the database of another agency and obtains information on whether there is any data on an individual (HIT) or not (NO-HIT). Depending on the results of such query, further information or cooperation between agencies can be requested. As such, in 2021, the EDPS participated, as an observer, in three meetings of the task force led by the Commission that is dealing with the implementation of a hit/no-hit functionality. This requires a coherent approach and interoperable IT solutions.

The fragmentation of the legal framework together with the interconnection of systems require the EDPS to adopt a holistic approach to the supervision of the AFSJ agencies and bodies. As the EDPS gained new supervisory powers, in 2021 the AFSJ sector was created, a dedicated Sector within the Supervision and Enforcement Unit of the EDPS. This newly created sector is dedicated to monitoring the processing operations of personal data linked to the core activities of the AFSJ agencies and bodies. The sector is responsible for ensuring that Regulation (EU) 2018/1725, and other data protection provisions specifically applicable to the AFSJ agencies and bodies, are interpreted and enforced consistently. With this new organisation, and taking account specific data protection rules, the EDPS was also able to tackle in a transversal and coherent way topics that affect several of the AFSJ agencies and bodies, such as the establishment of new cooperation instruments between Europol, Eurojust and the UK post-Brexit. The AFSJ Sector also continued to work closely with other Units at the EDPS, in particular the Technology & Privacy Unit, which provides the technical expertise required for the supervision of these agencies and bodies in different areas, such as artificial intelligence.

Another supervisory challenge consists in ensuring a close cooperation with national supervisory authorities as AFSJ agencies and bodies process personal data obtained from national authorities. To that end, we have actively participated in the different coordinated supervision bodies, in particular the Europol Cooperation Board, which is the advisory body established by the Europol Regulation; the [Cooperation Supervision Committee](#) that is established within the EDPB which addresses issues related to the supervision of EPPO and Eurojust; and the Supervision Coordinated Groups of the EU large-scale IT Systems.

## 4.2.

# Supervising Europol

**Europol** is the EU agency responsible for supporting the law enforcement authorities of the EU Member States in the fight against terrorism, and other serious and organised forms of crime.

The EDPS monitors and ensures the lawfulness of the processing of personal data by Europol, according to [Article 43](#) of Regulation (EU) 2016/794, the Europol Regulation.

The following subsections contain the annual report on the supervisory activities of Europol in accordance with Article 43 of the Europol Regulation.

Despite the extraordinary circumstances of COVID-19, in 2021 the EDPS returned to its inspection activities as carried out before the pandemic, while maintaining regular contact with Europol's management staff and other members of staff by organising, for example, bi-monthly meeting with Europol's data protection team and other members of staff.


## 4.2.1.

# The use of AI by Europol

The EDPS started the supervision of machine learning by Europol in 2019. Our work focuses on the use of operational data for the development, including training, testing, validation, and use of machine learning models.

We opened an own-initiative inquiry regarding Europol's use of operational data for 'data science purposes' - i.e. for the training, testing and validation of machine learning models. With this inquiry, we aimed to gain a better understanding of whether Europol intended to process or had already processed operational data for data science purposes, and whether these processing operations were compliant with the Europol Regulation.

We requested, on several occasions, detailed information about the policies in place; the appropriate legal basis for the processing operations; the safeguards put in practice to protect individuals' personal data; and



the specific projects that were at this point carried out by Europol. The replies and information sent to us were not considered satisfactory.

In parallel, in February 2021, Europol submitted a prior consultation on the development and use of machine learning models for the operational analysis of a big dataset in the context of a specific Joint Investigation Team (i.e. a specific cross-border criminal investigation) and Europol's support to the involved countries. Consequently, we decided to link this case to the inquiry and the annual inspection that followed.

We issued an opinion with 21 recommendations that Europol should follow in order to avoid possible breaches of the Europol Regulation. In particular, we suggested that Europol establishes an internal governance framework to ensure that, in the course of developing machine learning models, Europol identifies the risks to fundamental rights and freedoms posed by the use of these innovative technologies, even if Europol might not always be in a position to mitigate all of them, on the basis of the current state-of-the-art.

The development and use of such models was also one of the topics of Europol's Annual Inspection in September 2021. The inspection covered Europol's machine learning tool development process and the related data protection risk assessment process.

Given the importance of machine learning models for the performance of Europol's core tasks and the progress achieved in establishing an internal governance framework for artificial intelligence systems, we decided to allow the development of such tools upon the requirement that Europol puts in place specific measures and finalises the relevant data protection impact assessments.


#### 4.2.2.

### EDPS Annual Inspection of Europol

The EDPS carried out an onsite inspection on 27 and 28 September 2021 at Europol's Headquarters in The Hague, Netherlands.

The inspection focused on topics on which we had engaged actively with Europol since the end of 2020, including the use of artificial intelligence by Europol.





We audited three different areas that intersected with Europol's support to investigations related to the take down of three large criminal communication networks (Encrochat, SKY ECC and ANOM) over the last two years. We therefore looked at:

- Europol's data protection risk assessment process, and the way it is followed for these types of support operations in particular;
- Europol's machine learning tool development process;
- Europol's current operational structure, its current tools and its way of working with these datasets, in the absence of machine learning tools.

In a similar way as was done for previous inspections, we invited experts from national Data Protection Authorities (DPAs) to join our inspection. EU Member States are Europol's main information providers. As such, the participation of national experts in the inspection process helps to raise awareness of any problems arising at Europol level that might have originated at national level and how these can be addressed. For the inspection held in 2021, three experts from the DPAs of Germany, Croatia and the Netherlands participated in our inspection.

The inspection will result in an inspection report addressed to the Executive Director of Europol and shared with the Europol Cooperation Board.

#### 4.2.3.

### EDPS order to erase data concerning individuals with no established link to a criminal activity

On 3 January 2022, the EDPS [notified](#) Europol of an [order](#) to delete data concerning individuals with no established link to a criminal activity (Data Subject Categorisation). While the EDPS notified Europol of this Decision in 2022, the decision was taken in December 2021, and concludes the EDPS' inquiry launched in 2019.

In the context of its inquiry, the EDPS admonished Europol in September 2020 for the continued storage of large volumes of data with no Data

Subject Categorisation, which poses a risk to individuals' fundamental rights.

While some measures had been put in place by Europol since then, Europol had not complied with the EDPS' requests to define an appropriate data retention period to filter and to extract the personal data permitted for analysis under the Europol Regulation. This means that Europol was keeping this data for longer than necessary, contrary to the principles of data minimisation and storage limitation, enshrined in the Europol Regulation.

The EDPS was particularly concerned by the lack of definition of a maximum data retention period, which would have an impact on EU citizens and other individuals' rights whose data is in Europol's databases. The processing of individuals' data in an EU law enforcement database can have severe consequences for those concerned. Without putting in place the safeguards provided in the Europol Regulation, individuals run the risk of being wrongfully linked to a criminal activity across the EU, with all the potential damage to their private and professional lives that this could entail.

To this end, the EDPS decided to use its corrective powers and to impose a 6-month retention period for Europol to filter and to extract the personal data. A 6-month period for pre-analysis and filtering of large datasets enables Europol to meet the operational demands of EU Member States that are relying on Europol for technical and analytical support, while minimising the risks to individuals' rights and freedoms. Datasets older than six months that have not undergone this Data Subject Categorisation must be erased. This means that Europol is no longer permitted to retain data about people who have not been linked to a crime or a criminal activity for long periods with no set deadline. Furthermore, taking into account the operational needs of Europol and the amount of data collected so far, the EDPS granted a 12-month period for Europol to comply with the Decision for the datasets already received before this decision was notified to Europol.



#### 4.2.4.

### EDPS work on FIU.net

In 2021, the EDPS continued its work on FIU.net.

FIU.net is a decentralised information network designed to support national Financial Intelligence Units (FIUs) in their fight against money laundering and the financing of terrorism. FIU.net can also be used for the exchange of data on individuals involved in suspicious monetary transactions.

On 19 December 2019, we had issued a ban on the processing operations carried out by Europol regarding the technical operation of FIU.net. This decision was made because Europol was in breach of the Europol Regulation considering the restrictions on the categories of individuals' data that Europol is allowed to process.

The ban on Europol's processing operations concerning FIU.net was then suspended for an initial period of one year. This was done to ensure that Europol could carry out a smooth transition of FIU.net's technical administration to another entity, given the importance of combatting money laundering and terrorist financing at EU level.

Due to the complex nature of the FIU.net system and the large number of necessary steps to ensure a secure and stable transfer of the network, the EDPS decided to extend the ban until 30 September 2021.

However, we have been monitoring closely Europol's actions to ensure that the transfer of the technical administration of FIU.net to another entity is carried out safely, by requesting regular reports on their progress. In addition, we provided guidance and issued Opinions when necessary on specific issues encountered by Europol and the European Commission during this process.

We concluded our work concerning FIU.net's related ban on 15 October 2021, coinciding with the last report received by Europol, which confirms that Europol no longer operates as the technical administrator of FIU.net.



#### 4.2.5.

### Europol Decryption Platform

In December 2020, the EDPS opened an inquiry on the establishment of the updated Decryption Platform by Europol. This upgraded tool would allow Europol to provide more effective decryption support to EU Member States, when they require help with the decryption of static media collected during criminal investigations.

Our efforts focused on reviewing the details of the development and management of the tool, in particular regarding its hosting - a service through which storage and computing resources are provided to an individual or organisation for the accommodation and maintenance of one or more system(s).

We also reviewed the whole process of exchange of information for the operation of the Platform. We verified that the Platform did not involve specific processing of data presenting particular risks for individuals' rights and freedoms, which would require a prior consultation under [Article 39](#) of the Europol Regulation. EDPS consultations under Article 39 provide for an important safeguard, as it is a mechanism that allows the EDPS to be involved and green light new types of processing operations that present specific risks for individuals' fundamental rights, before they occur.

In 2021, we asked Europol to provide further information concerning the processing activities of the Platform and to facilitate a transparent analysis of the detailed procedures and processing of Europol regarding their decryption activities.

#### 4.2.6.

### Complaints made against Europol

In 2021, the EDPS received three new complaints from individuals against Europol and pursued its investigations concerning two complaints received in 2020.

According to the Europol Regulation, individuals are in principle entitled to obtain information on whether personal data relating to them is

processed by Europol. This right can be refused or restricted in case specific requirements apply, in the event that providing this information would not allow Europol to fulfil its tasks properly, or would jeopardise national investigations, for example. Europol is obliged to provide individuals reasons for which they cannot have access to the requested information within three months of receiving the individual's request.

The three complaints received in 2021 were from individuals who contested Europol's decisions to refuse access to their personal data. Reviewing complaints requires close cooperation between the EDPS and national Supervisory Authorities to carry out thorough investigations and to uphold individuals' data protection rights under the Europol Regulation.

While the overall number of complaints by individuals against Europol that we received remains low, these have increased compared to previous years. In addition, complaints are more substantiated and complex than those received in the past, requiring lengthy investigations.

When handling complaints according to [Article 47](#) of the Europol Regulation, we not only have to check data processing activities in Europol's systems, but national DPAs also have to check the lawfulness of the data transferred from national authorities to Europol, which can involve multiple authorities.


Furthermore, restrictions on travelling because of COVID-19 have also slowed down our investigations, because part of the required checks must be performed on Europol's premises.

#### 4.2.7.

### Opinions on individuals' right of access

We issued two Opinions in response to consultations by Europol relating to its obligations to handle individuals' requests to access their personal data.

The first Opinion, issued on 13 July 2021, provides guidance on how to handle repetitive access requests.



Under [Article 36\(1\)](#) of the Europol Regulation, individuals have the right to request, at regular intervals, whether Europol is processing personal data related to them. The Europol Regulation specifies that individuals have the right to submit their requests at “reasonable intervals”.


In the Opinion, we clarified the meaning of “reasonable intervals” and whether this corresponds to a specific timeframe. To establish whether the threshold of a reasonable interval has been exceeded, we recommended that Europol takes into account the circumstances in which a request is made and to way up the probability that circumstances surrounding the data processing operation may or may not have altered since the last request was submitted by the individual in question. As such, we highlighted that assessing the “reasonable interval” criterion has to be done by Europol on a case-by-case basis, rather than applying the one-size-fits all approach. Providing guidance on access requests submitted at “reasonable intervals” by individuals in our Opinion was particularly important because the Europol Regulation does not provide a procedure to inform individuals when the restriction of access to their data, in the context of ongoing criminal investigations for example, no longer applies. The only means available for an individual who has previously been refused access to their data to know that the restriction has been lifted, is to submit another request to access their data.

The second Opinion, issued on 13 December 2021, provides guidance on the scope of individuals’ access requests.

In our Opinion, we reiterated that no Europol system can be, in principle, excluded from a search when assessing individuals’ access requests.

Nevertheless, taking into account that some of Europol’s systems may be particularly complicated and burdensome to search because of the format or the unstructured nature of data, we requested that Europol puts in place appropriate measures to facilitate more efficient search and retrieval of data, and to make sure that individuals’ access requests can be properly reacted to.

We recalled that the right for individuals to access their data is a cornerstone of the fundamental right to data protection and is key to ensuring the fairness and lawfulness of processing.



#### 4.2.8.

### The processing of personal data of under 18s

In addition to the participation of national experts from the EU Member States' DPAs in Europol's Annual Inspection, and their involvement in investigating complaints made against Europol, the EDPS launched in 2021 an annual monitoring activity in the context of the Europol Cooperation Board.

Our joint-monitoring activity with the national DPAs focused on checking whether Europol and national competent authorities had put in place specific safeguards to protect individuals under the age of 18, in the context of criminal investigations for example, as provided under the Europol Regulation.

We paid specific attention to ensuring that personal data processed about individuals under 18 that are classified as suspects and "potential future criminals" in Europol's databases actually relate to individuals who have reached the minimum age of criminal responsibility, as set by the national law of the contributing EU Member States. This is particularly important for the processing of data about individuals that are under 15 years of age.

This 2021 joint-monitoring activity with national DPAs is a follow-up to an inspection the EDPS launched in 2018. During this 2018 inspection, we found that, because of the divergent and complex definition and interpretation of the minimum age of criminal responsibilities in EU Member States' law, Europol could not ensure that individuals below the minimum age of criminal responsibility were not labelled as suspects or potential future criminals in their databases, as this assessment was made by relevant authorities of EU Member States.

To this end, the 2021 joint-monitoring activity focused on specific checks of whether under 15s' data were lawfully shared with Europol.

Upon concluding this joint-monitoring activity, it was decided during a Europol Cooperation Board meeting in June 2021 that another annual joint monitoring activity would be repeated in 2022.

#### 4.2.9.

### Cooperating with the United-Kingdom after Brexit

Following the adoption of the [EU-UK Trade and Cooperation Agreement](#), the EDPS exchanged views with Europol concerning the establishment of a new cooperation instrument to be used between Europol and competent UK authorities, after the UK left the European Union ('Brexit').

To this end, we provided guidance on the data protection aspects of the Working and Administrative Arrangements foreseen between Europol and the UK, and on the supporting measures to put in place to carry out new arrangements between Europol and the UK.

#### EUROPOL STATISTICS

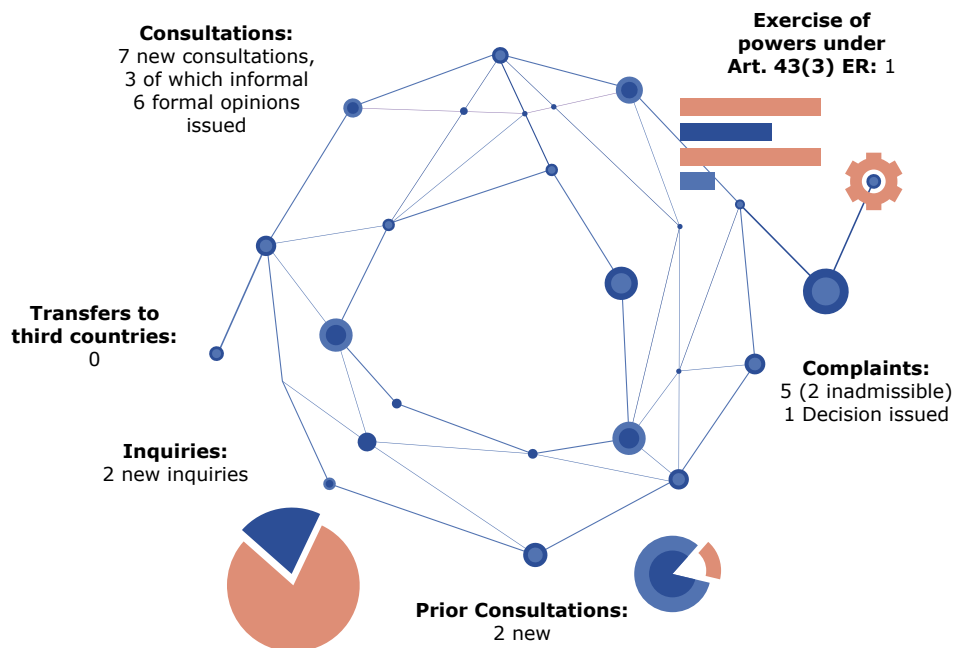


Figure 3: Europol Statistics 2021



### 4.3.

## Supervising EPPO

The European Public Prosecutor's Office ([EPPO](#)) became operational in June 2021, as an independent European body with the power to investigate and prosecute criminal offences against the European Union's financial interests.

This section represents the annual report on the supervisory activities of Europol in accordance with [Article 85\(5\)](#) of the EPPO Regulation.


Our work and efforts in 2021 focused on supporting EPPO to establish itself before it became operational, working closely with its data protection officer (DPO) by providing practical advice and recommendations.

Other examples of the support we provided to EPPO are detailed below.

In April 2021 an [external study](#), commissioned in 2020, was finalised. The objective of the study was to obtain legal analysis of EPPO's data protection framework to develop the EDPS' supervision strategy accordingly.

The results of the study confirmed the legal complexity of EPPO's supervision because of the heterogenic nature and structure of EPPO. Conclusions of the study also confirmed the need for close cooperation between the EDPS and the EDPB. As such, we further discussed EPPO's supervision within the Coordinated Supervision Committee of the EDPB to plan our work and cooperation for the future.

Another important step taken before EPPO became operational in June 2021 was the setting up of the Pre-Assessment Environment for the reports on criminal conduct submitted to EPPO by the general public. While most of EPPO's cases are received from national and European authorities, some reports are filed by citizens. These reports need to be filtered before a case is registered by EPPO. Therefore, in May 2021, we assessed the legality, necessity and proportionality of such pre-assessment environment and issued recommendations on its scope and risks for individuals' personal data that is described in the presented Data Protection Impact Assessment.



A few months after EPPO became operational and carried out its first few investigations, the Supervisor of the EDPS met with the European Chief Prosecutor, Ms Laura Kövesi, to discuss their ongoing and future cooperation.

As a follow-up to this exchange, various initiatives were organised in 2021, with some initiatives to be pursued in 2022; these include:

- an operational visit scheduled for 2022, which involves a visit to EPPO's premises;
- an address from the Supervisor to [the College of EPPO](#) to raise awareness of the EDPS' supervisory activities;
- a training session for EDPS colleagues on EPPO's case management system;
- an information session for EDPS colleagues on EPPO's external relations, with a particular focus on the exchange of operational and personal data.

#### 4.4.


### Supervising Eurojust

On 12 December 2019, a new supervisory framework for the processing of personal data at [Eurojust](#), the EU Agency for Criminal Justice Cooperation, came into force. Under the newly established Eurojust Regulation, the EDPS is responsible for monitoring Eurojust's compliance with the applicable EU rules on data protection.

This subsection contains the annual report on Eurojust in accordance with [Article 40\(5\)](#) of the Eurojust Regulation.

In 2021, the EDPS continued to work closely with Eurojust's DPO and other operational staff by providing them with informal advice when needed. Three meetings were held remotely between the EDPS and the DPO, discussing ongoing issues relevant to the processing of personal data by Eurojust.

Following the adoption of the [EU-UK Trade and Cooperation Agreement](#), we contributed to the fine-tuning of Eurojust's relations with competent UK authorities. The EDPS provided advice on practical data protection



questions and delivered opinions on the working arrangements between Eurojust and the UK's Home Office.

Finally, a first data protection audit, initially scheduled for 2020 and postponed due to the pandemic, took place in October 2021. The EDPS' audit focused on the processing of operational personal data by Eurojust and looked at data transfers in Eurojust's external relations; the functioning of the counter terrorism register and data security; and the use and performance of Eurojust's Case Management System, in particular. Following the onsite visit of the EDPS as part of the audit, we found that, overall; Eurojust's compliance with the data protection framework was satisfactory, with no critical compliance issues. However, some of the identified issues may be long term and may be linked to the outdated design and poor performance of Eurojust's case management system.

The EDPS invited the national supervisory authorities to make observations on this report before it becomes part of the annual report of the EDPS referred to in [Article 60](#) of Regulation (EU) 2018/1725.

#### 4.5.

### Supervising Frontex

In 2021, we continued our supervision of the activities of [Frontex](#), the European Border Coast Guard Agency, which contributes to the effective management of European borders.

Frontex's work involves the processing of personal data in various contexts, for example:

- when fighting organised cross-border crime and terrorism at the EU's external borders in cooperation with Europol and Eurojust;
- setting up and running the central unit of the European Travel Information and Authorisation System ([ETIAS](#)) to determine whether non-EU nationals pose a threat to the security of the EU;
- supporting EU Member States to manage their external borders.

To provide support to Frontex as they put in place data protection safeguards, we developed in 2021 a solid collaboration and working relationship with the DPO of Frontex, by holding regular bilateral meetings

and consultations. These meetings aimed to gain a better understanding of Frontex's structure and core activities under the new [Frontex Regulation](#) to determine the EDPS' strategic supervisory activities for 2022. The consultations covered numerous topics, such as the status, role and tasks of Frontex's DPO, as well as the continued application of rules adopted under the former Frontex Regulation.

We also provided guidance on Frontex's activities in assisting EU Member States when returning migrants - who do not fulfil the conditions for staying in the EU - are sent back to their home country. In particular, we gave our advice on the technical tools Frontex and EU Member States are using in this context, and provided [advice](#) on the transfers of personal data about these migrants by Frontex to non-EU countries.

#### 4.6.

### Supervision of large-scale IT systems

As part of our supervisory work, we are responsible for supervising the processing of personal data in the central units of large-scale IT systems in the field of Justice and Home Affairs. We also ensure that the development of such systems complies with the principles of data protection by design and default.


The supervision of large-scale IT systems requires we cooperate with EU Member States' DPAs, through the Supervision Coordination Group (SCGs), to ensure coordinated end-to-end supervision of all databases.

#### 4.6.1.

### Supervision of eu-LISA

While we supervise the EU's large-scale IT systems from a data protection perspective, three of these systems - [Schengen Information System](#), [Visa Information System](#), and [Eurodac](#) - are managed by eu-LISA, the EU Agency for the Operational Management of Large-Scale IT systems in the Area of Freedom, Security and Justice.

Within its role, eu-LISA supports EU policies on asylum; border management; police cooperation and migration, by allowing EU Member States' authorities, and some EU bodies, to exchange information relating



to borders; migration; and police investigations. With the development of new large-scale IT systems managed by eu-LISA, such as the Entry/Exit System ([EES](#)), the European Travel Information Authorisation System ([ETIAS](#)) and the European Criminal Records System - Third Country Nationals ([ECRIS-TCN](#)), our supervision activities are increasing given their heightened impact on individuals' right to the protection of their personal data.

In light of these circumstances, we organised regular meetings in 2021 with eu-LISA's DPO, and other members of staff involved in the processing of data in their day-to-day work, which allowed us to help them address issues detailed below.

### 1. The European Travel Information Authorisation System

We were consulted in June 2021 by eu-LISA on their [Data Protection Impact Assessment](#) regarding the European Travel Information Authorisation System (ETIAS), a large-scale information system that will make advanced security checks of visa-exempted travellers to determine:

- whether they pose a security or health risk;
- to flag irregular immigration;
- whether they are allowed to enter the Schengen area.

Upon examining the facts, we concluded in our Opinion that the DPIA was not sufficiently developed to provide a precise and comprehensive identification and assessment of the risks of ETIAS for individuals' fundamental rights.

To this end, we highlighted that it was necessary to include in the DPIA:

- the risks related to the interactions of the system with processing operations that are under the responsibility of other stakeholders, such as Frontex, Europol and the EU Member States;
- to provide a clear description of the whole system to facilitate the identification of high-level related risks; and
- to ensure that for each specific risk that is identified, the source, the impact and the mitigation measure are described.

We also provided guidance on how to develop a DPIA in order to ensure a full assessment of the impact of the envisaged processing operations on the fundamental rights of individuals.

## 2. Shared Biometric Matching Service

In July 2021, we were consulted on the Shared Biometric Matching Service (sBMS), which will store and match individuals' biometric data, such as their fingerprints, facial images, under specific conditions, and aims to facilitate the exchange of biometric data between different large-scale IT systems, such as the Schengen Information System (SIS) and the Visa Information System (VIS). The sBMS will be used for the first time when the future Entry Exit System (EES) becomes operational to search if the person passing the EES gate is listed in VIS.

Eu-LISA conducted a DPIA for the sBMS and identified high risks which could not be mitigated, and therefore proceeded to consult us, according to [Article 40](#) of Regulation (EU) 2018/1725 on prior consultations. We provided our feedback on 4 November on the DPIA, as well as on eu-LISA's request to use real biometric data from the VIS database, to measure the performance of the matching algorithms.

## 3. Updated Policy on Personal Data Breaches

On 2 July, we provided an Opinion on eu-LISA's updated policy on personal data breaches. This policy provides the main guidelines and definitions on how to handle personal data breach incidents, a framework to assess the impact of a data breach, and the roles, responsibilities, and requirements of those who are involved in the processing of personal data or personal data breach.

## 4. Updates on SIS II, VIS and Eurodac Inspections

Following our inspections of SIS II, VIS and Eurodac, eu-LISA continued to provide us with regular feedback on how it puts in place the recommendations we issued as a follow-up. Equally, we provide support and further guidance if necessary when some recommendations are not correctly put in place to ensure that individuals' data is protected according to Regulation (EU) 2018/1725.

#### 4.6.2.

### Supervision Coordination Groups of large-scale IT systems

Due to the pandemic, the [Supervision Coordination Groups](#) (SCGs) for Eurodac, the SIS, and the VIS met remotely in June and November in 2021; the SCG for the Customs Information System (CIS) met remotely in June 2021.

We attended these meetings and took on an active role within these groups. As an example, in 2021, we contributed to the discussions within the VIS SCG on the nature, scope and content of a common security audit framework within the Group, which would help DPAs perform inspections of VIS, and in particular inspections on the information security aspects of the system. We played an active role in developing the technical part of the common audit.


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

An abstract graphic on a dark blue background featuring a network of light blue dots connected by thin lines, creating a web-like pattern. The dots and lines are more concentrated on the left side and fade out towards the right.

## **CHAPTER FIVE**

# **Technology and Privacy**





Data protection has a strong connection with technology. Technology developments will make society advance, and increase the well-being of individuals. At the same time, some of these advances have the potential to increase and/or exacerbate privacy and data protection risks. DPAs must be aware of the potential risks and opportunities presented by technological advances. DPAs should invest time in understanding the possibilities of new technology, while also encouraging the integration of data protection by design and data.

We place strategic importance on integrating the technological dimension of data protection into our work. This work is undertaken by Technology and Privacy Unit (T&P) of the EDPS. T&P monitors, advises and acts upon technological developments and trends through various initiatives, some of which are detailed below.

#### 5.1.


### TechDispatch receives an award

The aim of the [TechDispatch reports](#) is to explain, inform and raise awareness of potential data protection issues surrounding new technologies. Each TechDispatch provides factual descriptions of a new technology, assesses its possible impact on privacy and personal data protection, and provides links to further recommended reading. We hope to contribute to the ongoing discussion on new technologies and data protection with these reports.

In October 2021, our TechDispatch initiative received the [Global Privacy and Data Protection 2021 Award](#), for the “Education and Public Awareness” category at the 43rd Global Privacy Assembly 2021.

The [Global Privacy Assembly](#) is an international forum for data protection and privacy authorities. The GPA Awards celebrate the achievements of the GPA community and rewards good practices adopted in the privacy and data protection fields. As such, the Supervisor and our EDPS colleagues appreciate the recognition received for our commitment to inform the public of new technologies and data protection.

In 2021, we published two issues of the TechDispatch: one on Facial Emotion Recognition, and one on card-based payments.



#### 5.1.1.

### Facial Emotion Recognition

In this [TechDispatch](#), the T&P unit explored the data protection implications of Facial Emotion Recognition (FER) in May 2021. FER is a technology that analyses facial expressions from static images and videos to reveal information on a person's emotional state. Although FER can be used for a variety of purposes, this technology comes with several data protection implications and concerns. This issue explores whether the use of FER generates accurate data, whether processing data with FER is necessary and proportional for the purpose envisaged and whether FER discriminates on grounds of skin colour or ethnic origin.

#### 5.1.2.

### Card-based payments


Published in December 2021, this [TechDispatch](#) explores the data protection issues and challenges with card-based payments. Consumers and businesses are looking for a simpler, personalised, and economically feasible way of conducting day-to-day transactions. Cash payments are increasingly being replaced by cashless payments via an ever-growing landscape of emerging solutions, such as contactless payments using Near Field Communication (NFC), or Quick Response (QR) technologies, or cardless payments via smartphone apps. This report explores multiple issues associated with card-based payments like data retention, security and the processing of special category data.

#### 5.2.

### Our new initiative: TechSonar

On 28 September 2021, the EDPS launched a new initiative, [TechSonar](#). Our TechSonar report aims to anticipate emerging technology trends to better understand their future developments, especially their potential implications on data protection and individuals' privacy.

In a [blogpost](#) explaining the philosophy of the TechSonar reports, the Supervisor of the EDPS, Wojciech Wiewiórowski, emphasises the need to act in advance and to anticipate the developments of technology trends



to ensure that data protection and privacy features are embedded in these emerging technologies, from the earliest stages of their conception.

In the first [EDPS TechSonar 2021-2022 report](#), in addition to identifying methodological aspects, technology experts from the EDPS have chosen to explore the following six foreseen technology trends:

- Smart vaccination certificates;
- Synthetic data;
- Central bank digital currency;
- Just walk out technology;
- Biometric continuous authentication;
- Digital therapeutics.

For each trend, the TechSonar report includes information about what this technology may involve, its impact on our day-to-day lives and possible implications on individuals' privacy, both the positive and negative aspects.

### 5.3.

## Personal data breaches

Under Regulation (EU) 1725/2018, all European institutions, offices, bodies and agencies (EUIs) have a duty to report personal data breaches to the EDPS, unless a risk to the affected individuals is unlikely.

A personal data breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, transmitted, stored or processed personal data.

This type of breach may affect the confidentiality, integrity or availability of personal data. Breaches can be caused due to several reasons, for example, when an electronic device containing non-encrypted personal data is lost. The implications of a breach can be serious, such as identity theft or damage to reputation.

All EUIs must notify the EDPS of the breach within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to pose a high risk of adversely affecting individuals' rights and freedoms, the EUI in

question must also inform the concerned individuals without unnecessary delay. If the EUI concerned is delayed in notifying the breach, this should be explained. If not all information is available regarding the incident, the EUI in question should notify the breach in phases. There are similar obligations applying to [Europol](#) under Regulation (EU) 2016/794, and the [European Public Prosecutor's Office](#) under Regulation (EU) 2017/1939.

Risk assessment is a core element in preventing and responding to personal data breaches. Unlike other traditional risk assessment methodologies, the focus of a personal data breach is on evaluating the risk to the rights and freedoms of individuals. While various stakeholders, supervisory authorities, private and public organisations use a range of different methodologies to do this, our data breach [Guidelines](#) aim to simplify this task by providing guidance and practical examples to assist EUIs in their efforts. In 2021, we also contributed to the finalisation of the [EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification](#), following the public consultation process.

As part of our work, we support EUIs by raising awareness of personal data breaches and on how to prevent these from happening, and helping EUIs with their obligations in the event that a personal data breach does occur.

### 5.3.1.

## Raising awareness of personal data breaches

In 2021, we continued our efforts to raise awareness of personal data breaches. We have found in past years that two of the effective ways of doing this is by sharing factsheets, videos, as well as organising talks and short training sessions periodically. Some of these initiatives are detailed below.

In May 2021, we published a [factsheet](#) and its accompanying [video](#) on personal data breaches in English, French and German on the EDPS website. Both the video and the factsheet aim to provide an overview to EUIs of the type of personal data breaches that may happen, how to prevent these breaches from happening, and what to do if a breach still happens. The factsheet and video can also provide an overview of personal data breaches to other entities processing personal data within the EU, such as public administrations, that must follow similar procedures and notify their national data protection supervisory authorities.

Following the publication of the factsheet and video on personal data breaches, we also delivered an online talk, hosted by the European School of Administration, for staff members of EUIs, on personal data breaches and data breach notifications, on 9 November 2021. With more than 150 participants attending the online talk, discussions delved deeper into the common data breaches that occur in EUIs, including errors in postal mail or emails, technical errors and the effects of external cyber-attacks. Mistakes related to handling and assessing personal data breaches, and the measures to put in place to both prevent and address personal data breaches were also at the heart of the online talk.

The EDPS also organised a dedicated session on personal data breach notifications during the 49th meeting with the network of DPOs from EUIs ([see Chapter 3](#)). The outcome of this session will be taken into account when updating the EDPS guidelines on personal data breach notification.

### 5.3.2.

## Data breach statistics

In 2021, the EDPS received and assessed 87 new personal data breach notifications under Regulation (EU) 2018/1725.

Compared to the 121 personal data breaches received in 2020, there was a 28% decrease of the number of personal data breaches notified to the EDPS this year.

### Data Breach Notifications per month 2021

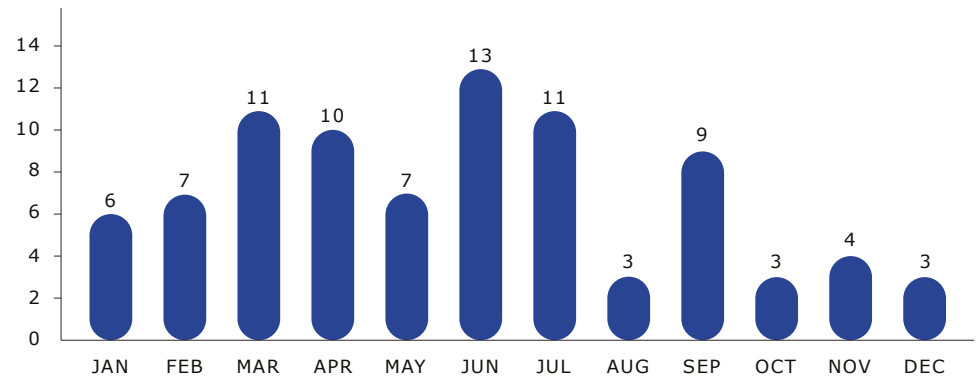


Figure 4: Number of Personal Data Breach Notifications per month in the year 2021

### Personal Data Breach Notifications 2019-2020-2021

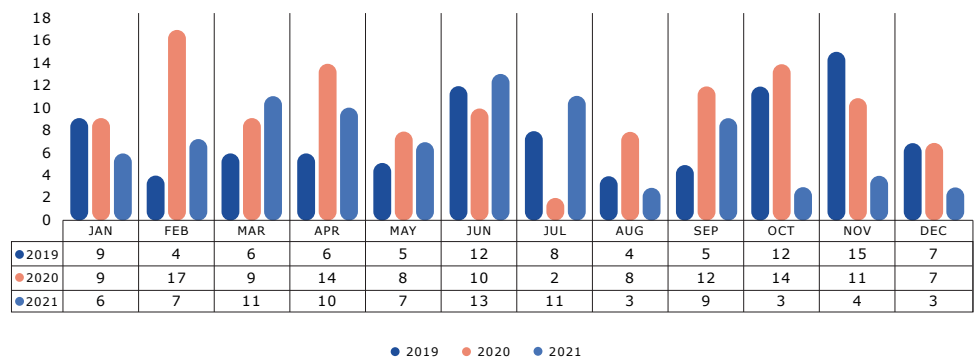


Figure 5: Number of Personal Data Breach Notifications per month for the years 2019-2021

### 5.3.3.

## Root Cause of Personal Data Breaches in 2021

Upon examining the personal data breaches that were notified to us, human error remained the most common root cause of personal data breaches in 2021, with an increase of 9% in comparison to 2020. The most common situation in which personal data breaches occurred includes the sending of emails to the wrong recipients, or putting all recipients in copy when these should have been in bcc for example.

We also received data breach notifications concerning documents that were published without removing individuals' personal data in the context of EUIs' access and transparency procedures.

Similar to 2020, this year was marked by a high number of human errors during recruitment procedures because EUIs continued to hold these procedures online.

The second most common cause amongst the personal data breaches notified to us in 2021 were external attacks, although the underlying reasons of the attacks and their success varied. The attacks may have resulted from zero day vulnerabilities being exploited, from the lack or ineffective security measures or even due to users not being aware, or being partially aware, of the measures to protect themselves from malware and phishing attacks for example.

Personal data breaches due to external attacks are on the rise, especially after the start of teleworking due to COVID-19. These external attacks usually affect larger numbers of individuals compared to human errors.

This is because an external attack could allow the access to full databases or systems, in which data about different individuals stored. The rise of personal data breaches follows a general trend of increased cyberattacks.

Since external attacks have increased in 2021 - including attacks possibly exploiting personal information stored in the information systems of the EUIs - it may require all EUIs to review and strengthen their information security measures.

Furthermore, data breaches caused by technical error decreased by 7% in 2021, compared to 2020. The most common type of technical error is when someone is provided with access to documents they should not have had access to.

## Type of Personal Data Breaches 2021

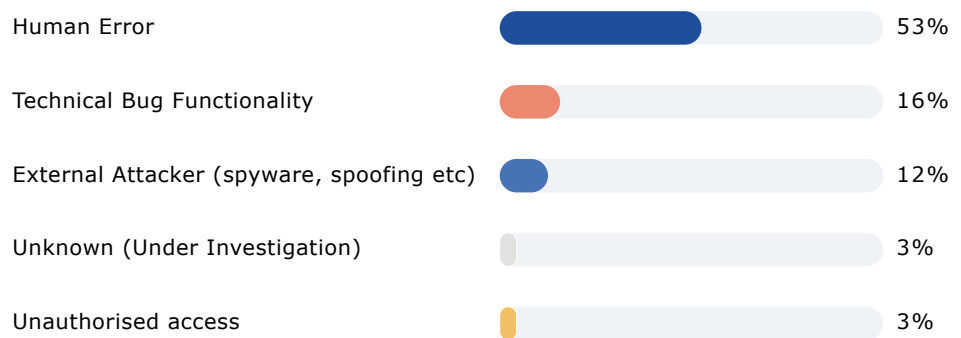


Figure 6: Root Cause of the Personal Data Breaches 2021

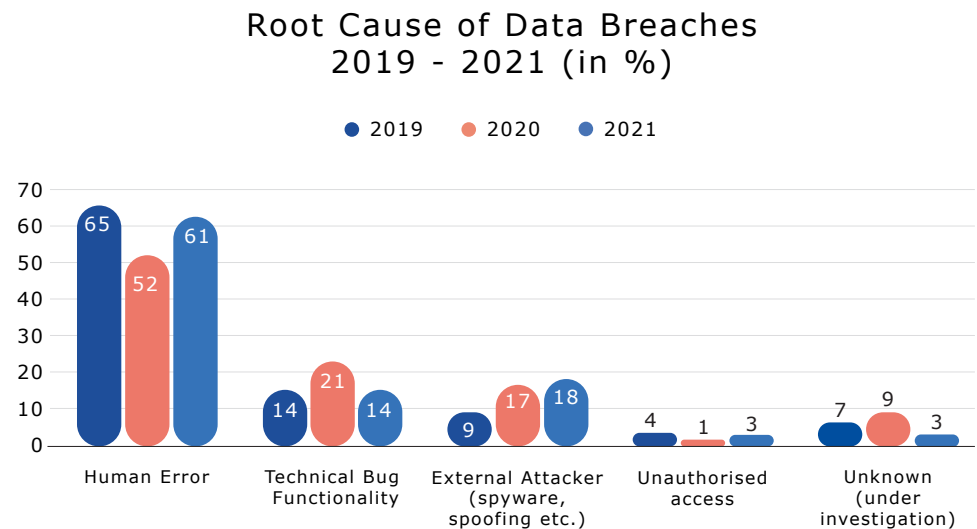


Figure 7: Comparison Chart on the Root Cause of the Personal Data Breaches 2019-2021



#### 5.3.4.

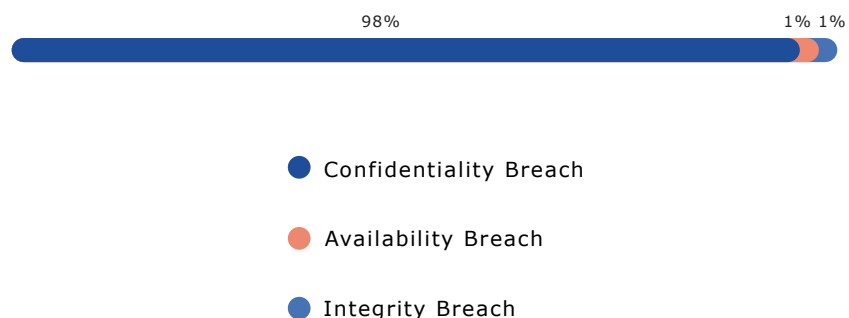
### Type of Personal Data Breaches in 2021

A personal data breach results from either one of the type of breaches explained below, or a combination of them:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, personal data, which is about getting knowledge of personal data by an entity not entitled to this knowledge.
- **Availability breach** – where there is an accidental or unauthorised loss of access to, or destruction of, personal data, which is about losing control of access to personal data, or inappropriate deletion of personal data.
- **Integrity breach** – where there is an unauthorised or accidental alteration of personal data, which is about inappropriate modifications of personal data.

The vast majority of notified personal data breaches in 2021 concerned a breach of confidentiality (98%).

### Type of Personal Data Breaches Year 2021



*Figure 8: Type of Personal Data Breaches*

In 2021, we received 50 complete data breach notifications and 37 notifications in phases. EUIs notified the breaches in phases by providing initial information and an assessment to the EDPS when they cannot provide all the necessary information concerning a personal data breach within the time frame of the 72 hours from when they became aware of the breach. EUIs then need to provide follow-up notifications with updated assessments when they are able to further analyse the breaches and its impact on individuals. Until the end of 2021, not all notifications in phases were finalised on the EUI's side. As shown below, the proportion of comprehensive notifications and notifications in phases did not differ significantly compared to previous years.

Type of Personal Data breach Notifications 2021

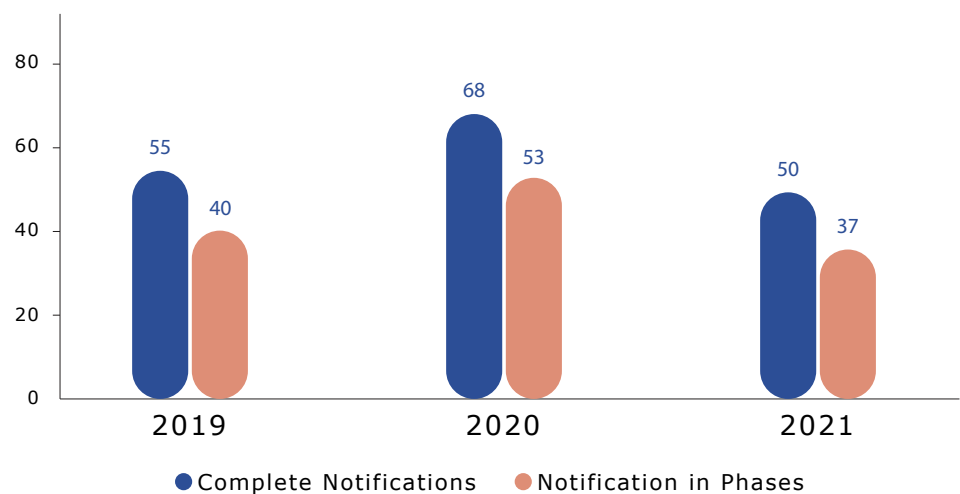


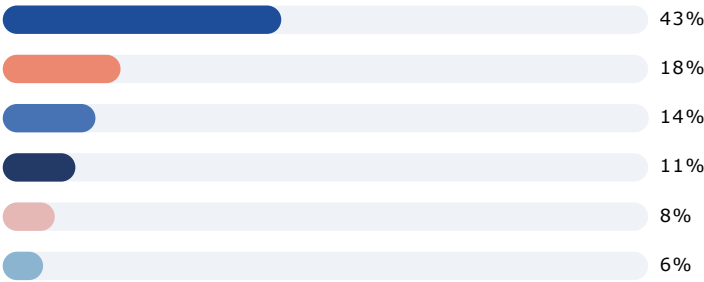
Figure 9: Type of Data Breach Notification

5.3.5.

Number of affected individuals of  
Personal Data Breaches in 2021

Regarding the number of affected individuals of the notified personal data breaches, in the majority of cases (43%) a small number of individuals (1-10) were affected, while in 18% of the cases, 11-50 individuals were affected. In 12 cases of personal data breaches, more than 1000 individuals were affected, which equals to 14% of the total cases.

Affected Individuals per Notification 2021



	1-10	11-50	51-100	101-500	501-1000	1000 and more
Notifications	43%	18%	6%	8%	11%	14%

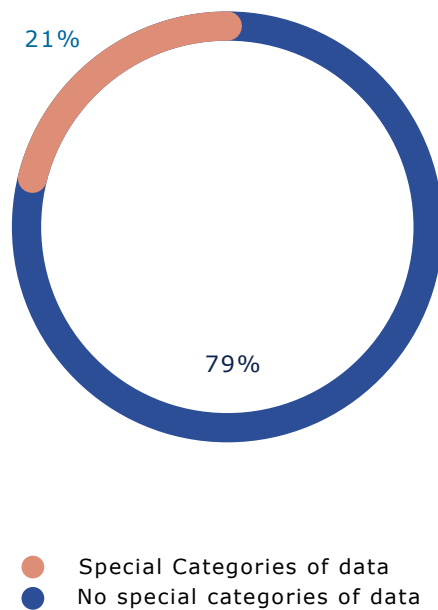
Figure 10: Impact of Personal Data Breaches

### 5.3.6.

## Special Categories of Data in Personal Data Breaches in 2021

Amongst the personal data breaches that were notified to us, 23% of these involved special categories of data; this includes health data, personal data revealing racial or ethnic origin to name a few examples.

### Special Categories of Data in Personal Data Breaches in 2021



*Figure 11: Special Categories of data in personal data breaches notifications*

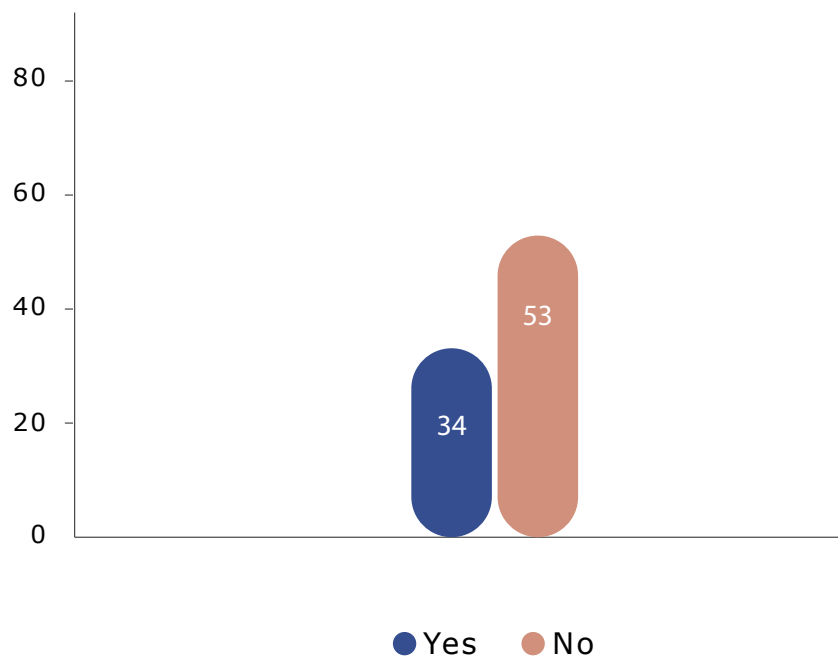
### 5.3.7.

## Notification to individuals in 2021

In 34 cases, EUIs decided to notify the personal data breach to affected individuals. While some were obliged to do so due to the high risks identified for individuals, other EUIs decided to notify individuals of the breach as a matter of transparency.

We recognise and value EUIs that are transparent about personal data breaches on a voluntary basis. A typical example of this is, when EUIs communicate a data breach to individuals on a voluntary basis when they occur in the context of recruitment procedures.

## Notification to the Data Subjects 2021



*Figure 12: Notification to the Data Subject*

Upon receiving a data breach notification from an EUI, we immediately and systematically assess these by often submitting additional requests to the EUIs' controllers; this includes asking for clarifications or for more



information on the breach, as well as making suggestions on possible mitigation actions to lower the risks for the affected individual(s).

Similar to previous years, we received in 2021 notifications outside of our competence.

For 6 of these notifications received from EUIs where we were not competent, we assessed that these breaches were unlikely to present risks for individuals. We therefore advised EUIs to simply document the breach in their internal register.

We also received 7 notifications of personal data breaches from private companies or individuals, as whistle-blowers, which were outside the scope of the Regulation (EU) 2018/1725, and therefore outside of our competences. These breaches were either from companies having a main establishment in the EU - in which case the national Supervisory Authority under GDPR would be competent - or from companies processing data of EU citizens, without an establishment in the EU.

#### 5.4.


## Cooperation with data protection authorities in technology and privacy matters

The EDPS regularly collaborates with other data protection authorities within the European Union. The aim of these collaborations is to exchange information on best practices related to data protection and privacy matters, raise awareness of certain technologies that have an impact on data protection for individuals, public administrations and companies, and to support and improve cooperation between various data protection authorities.

#### 5.4.1.

### Myths on Data Anonymisation

On 27 April 2021, we published together with the Spanish Data Protection Authority, Agencia Española de Protección de Datos (AEPD), a Joint Paper on "10 misunderstandings related to anonymisation". The process of



anonymising personal data ensures that the individual to whom this data relates to is not, or no longer, identifiable. With this paper, the EDPS and the AEPD aim to bring clarity on what data anonymisation means and contribute to clearing up some misconceptions surrounding this topic. Some misunderstandings related to data anonymisation discussed within the paper are:

- anonymisation is forever.
- anonymisation of data is always possible.
- anonymisation is a binary concept that cannot be measured.

To find out more about the myths linked to data anonymisation, read the EDPS-AEPD Joint Paper in English: "[10 misunderstandings related to anonymisation](#)" or in Spanish: "[10 malentendidos relacionados con la anonimización](#)".

#### 5.4.2.

### The "Berlin Group" in 2021

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

The IWGPT was established in Germany in 1983, and is composed of technical, legal and regulatory experts from Data Protection Supervisory Authorities, including the EDPS, Non-Governmental Organisations and academia around the world.

In 2021, the IWGDPT met online twice. The German Federal Commissioner for Data Protection and Freedom of Information formally took over the chair of the group in March 2021. During these meetings, the IWGDPT adopted a [Working Paper on the Role of Data Portability](#) and a [Working Paper on the Risks emerging from the Tracking and Targeting Ecosystem Established for the Digital Advertising Market](#).

The Group is currently working on a paper on sensor networks, which will be proposed for adoption soon, and has also decided to explore if work on voice-controlled devices is needed, and envisages to prepare papers on smart cities, and facial recognition technology.

The Privacy Protection Authority of Israel and the UK Information Commissioner have offered to host meetings in their countries in 2022.

5.5.

## Cybersecurity training session for EDPS colleagues

In March 2021, the EDPS' and the EDPB's Local Information Security officers organised a remote cybersecurity training session for the EDPS and the EDPB staff in collaboration with [CERT-EU](#), the Computer Emergency Response Team for European institutions, bodies and agencies.

The purpose of the session was to raise awareness about possible cybersecurity threats and how the EDPS and the EDPB staff can protect themselves, their institution, as well as other individuals against such threats, especially in times of teleworking.

With the use of interactive presentations and exercises, all staff were given an overview of:

- the different types of hacking methods used, such as phishing, smishing and vishing.
- the motivations behind hacking attempts, what hackers are looking for, and why staff can be a target.
- how to recognise hacking attempts based on the content of an email, links included in an email and the author of an email, for example.

CERT-EU colleagues also gave staff some tips on how to better protect their personal data by creating stronger passwords, using multi-factor authentication methods to secure email accounts, and encrypting their data for example.

The EDPS and EDPB Local Information Security Officers will continue to collaborate with each other to ensure that staff have the necessary tools to protect their personal data.



5.6.

## IPEN workshops

In 2021, we continued to organise the EDPS' IPEN workshops and webinars. Founded in 2014, the [Internet Privacy Engineering Network \(IPEN\)](#) brings together experts from a range of different areas to encourage the development of engineering solutions to privacy problems.

By facilitating exchanges between regulators, researchers and developers who build privacy into new and existing digital tools, our IPEN initiative aims to promote and advance state of the art practices in privacy engineering.

We held two IPEN webinars in 2021, one on Synthetic Data and one on pseudonymous data.

5.6.1.

### Webinar on synthetic data

The chosen topic of the [EDPS' IPEN webinar workshop](#) in June 2021 explored the role that synthetic data may have in the context of data protection. Synthetic data is the ability to create new artificial data based on an individual's personal data while keeping similar statistical properties to ensure that it can still be useful in context. This webinar was attended by 170 expert practitioners and professionals in the data protection and privacy field and focused on the use of synthetic data instead of real data as an applied privacy measure in certain domains (mostly healthcare) and in specific use cases, such as AI and data science projects, or software testing, and simulations for technology assessments. Discussions touched on the benefits and challenges of using synthetic data instead of original data to protect individuals' privacy. Guest speakers agreed that the main challenges are, whether synthetic data can still be useful for set purposes in the same way as original data belonging to individuals would be, and whether synthetic data is a sufficient measure against privacy attacks.

To find out more, read the [EDPS' Blogpost](#) and watch the [video recordings of the event](#).



### 5.6.2.

## Webinar on pseudonymisation

The [second IPEN webinar workshop](#), held on 9 December 2021, was on pseudonymisation as a foundational technique to mitigate data protection risks.

According to the EU's personal data protection legislation, pseudonymisation is the processing of personal data in such a way that it is no longer attributed to a specific individual, without the use of additional information. During our webinar, we focused on the practical use of pseudonymisation techniques to mitigate data protection risks when processing personal data. Our aim was to provide an opportunity to increase awareness on existing guidance, explore options and challenges, and offer organisations an understanding of the tools and advice available to implement pseudonymisation effectively.

The video recordings and speakers' presentations of each session are available on the [IPEN webinar webpage](#).

### 5.7.


## Digital sovereignty and digital transformation

### 5.7.1.

## EDPS IT gap analysis

On 30 June 2020, the EDPS presented its [Strategy 2020-2024](#). Our strategy describes how we intend to carry out our obligations as the data protection authority of EUIs, and how to deploy resources to address these challenges. More specifically, the Strategy aims at enabling the EDPS to support EUIs to continue to lead by example in safeguarding digital rights and responsible data processing.

We therefore launched a two-phase project towards a digital transformation of the EDPS, based on the objectives set out in our Strategy.



In 2021, we accomplished the first phase, called IT Gap Analysis. We analysed the current IT needs of the EDPS and mapped existing IT tools and systems to be able to identify possible gaps, based on interviews with various members of the EDPS staff and other identified stakeholders. The outcome included a description of the way forward to cover the gaps and criteria to identify relevant solutions. The IT Gap Analysis is a starting point for the second phase of the digital transformation project. In 2022, we envisage launching an IT feasibility study to assess possible options for a new EDPS IT infrastructure that best fits EDPS needs, based on necessary resources and policy alternatives.

#### 5.7.2.

### Digital Sovereignty panel for CPDP 2021

We organised a panel for the Computer, Privacy & Data Protection (CPDP) conference, titled "Enhancing Personal Data Protection through Digital Sovereignty", on 27 January 2021. CPDP is a non-profit platform that gathers academics, lawyers, practitioners, policymakers, industry and civil society experts from around the world to discuss developments within the privacy and data protection field. Our panel addressed the following issues:

1. The progress of, and public and private sector support for, EU sovereign Infrastructures?
2. What instruments do we need for Digital Sovereignty?
3. How can EU entities develop Insourcing strategies for innovation in the EU?
4. How could Digital Sovereignty benefit privacy and the protection of personal data?

Panellists discussed the interplay between digital sovereignty and data protection, and the need to offer compliant and competitive, user-friendly services. Based on concrete examples, the feasibility of insourcing and the use of free software alternatives was explored.

There are multiple benefits from attending these panel discussions. Firstly, they offer an opportunity for DPAs, such as the EDPS, and other experts in the privacy and technology field to exchange views and possible solutions and improvements to ensure that technological progress goes

alongside the protection of individuals' data. We also get to explore new initiatives. Finally, by inviting a variety of experts, it is a chance for us to learn more about what works from a practical perspective.

5.8.

## Website Evidence Collector 1.0

In 2021, we continued to work on the EDPS' [Website Evidence Collector](#) (WEC), originally launched in 2019. Our efforts meant that we were able to release the WEC's 1.0 version on 12 January 2021.

The WEC is a tool that collects evidence of personal data processing, such as cookies, or requests to third parties on websites. DPAs, data controllers and web developers can use the WEC to carry out their own website inspections and better understand what type of information is stored during a website visit.

The WEC's 1.0 version includes several new configuration options to allow, for example:

- virtualisation.
- browsing with the [Do Not Track](#) activated.
- custom browser profiles or pre-installed cookies.

In addition, the documentation was extended to cover examples on how to carry out data evaluation.

The EDPS' WEC is published as open source software under the European Union Public License (EUPL-1.2); the software is available for download via the [EDPS' website](#), on the European Commission's [collaborative platform Joinup](#) and on the popular developer platform [GitHub](#).

As part of our efforts to improve the Website Evidence Collector, we welcome all contributions in the form of ideas, bug reports or code. Feedback and suggestions for improvements can be sent to: [tech-privacy@edps.europa.eu](mailto:tech-privacy@edps.europa.eu)

[Download the EDPS' Website Evidence Collector now!](#)

5.9.

## Eurodac Inspection Report

In March 2021, the EDPS issued its inspection report on [Eurodac](#), a European Union database that identifies asylum seekers applying for international protection by collecting their fingerprint data.

In the inspection report, we made several recommendations addressed to the European Union Agency for the Operational Management of Large-Scale IT Systems ([eu-LISA](#)), the European Union agency in charge of the operational management of Eurodac.

We addressed several recommendations to eu-LISA, including on the Eurodac-Central System and on the retention periods of storing fingerprints in the system according to [Articles 12\(2\)](#) and [16\(1\)](#) of the Eurodac Regulation (EU) No 603/2013. In our report, we reiterated several of the recommendations made during its previous inspection in 2016, which were not yet implemented by eu-LISA. The report was also sent to the European Parliament, the European Council, the European Commission, and the national supervisory authorities in the Member States.

As the independent data protection authority for EUIs, we will continue to monitor whether eu-LISA follows the recommendations set out in the report within the set deadlines.

Our report and findings are routinely presented to the DPAs in our regular meetings with [Eurodac Supervision Coordination Group](#).

The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting small, semi-transparent blue dots. These dots and lines are scattered across the page, creating a sense of interconnectedness and a modern, technological feel. The lines and dots are more concentrated in some areas, particularly around the text, and more sparse in others.

## **CHAPTER SIX**

# **Legislative Consultations**

The EDPS serves as advisor to the EU legislator on all matters relating to the processing of personal data. We provide guidance on proposed legislation to the European Commission as the institution with the right of legislative initiative, and to the European Parliament and the Council as co-legislators.

Our guidance may take different forms, detailed below.

- **Opinions** - Our [Opinions](#) are issued in response to mandatory requests by the European Commission, which is legally obliged to seek our guidance on any legislative proposal, or draft implementing or delegated acts, as well as recommendations and proposals to the Council in the context of international agreements with an impact on data protection. [See Annex D.](#)
- **Formal Comments** - Similar to our Opinions, our [Formal Comments](#) are issued in response to a request from the European Commission and address the data protection implications of legislative proposals. However, they are usually shorter and more technical, or only address certain aspects of a proposal. [See Annex E.](#)
- **Informal Comments** - The European Commission is encouraged to consult us informally before adopting a proposal that has an impact on data protection. This allows us to provide the European Commission with input at an early stage of the legislative process, usually at the stage of the inter-service consultation.
- **Joint EDPS-EDPB Opinions** - Where a legislative or other relevant proposal is of particular importance for the protection of personal data, the European Commission may also consult the European Data Protection Board (EDPB). In such cases, the EDPS and EDPB work together to issue a joint opinion. [See Annex F.](#)

The statutory deadline for us to provide advice in the context of a legislative consultation is eight weeks.

In addition, we meet annually with legislative and data protection coordinators from across the European Commission to discuss the Commission Work Programme and identify initiatives that are likely to require our consultation.



6.1.

## An increase in Informal and Formal Legislative Consultations


Since the entry into application of Regulation (EU) 2018/1725, the number of requests for legislative consultation has significantly increased. In 2019, we answered a total number of 35 requests for legislative consultation, whereas in 2020 the number of legislative consultations increased to a total of 50. In 2021, the EDPS responded to **88 formal legislative consultations** pursuant to [Article 42\(1\)](#), including 12 Opinions and 76 Formal Comments. In addition, **5 Joint Opinions** were adopted with the EDPB pursuant to Article 42(2) EUDPR. This steep increase in consultations can be attributed to a variety of different factors, explained below.

**1) An increase in legislative initiatives** - There has been an increasing number of legislative initiatives containing provisions that have an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data. There has therefore been an increase in the number of institutions and organisations that have contacted the EDPS for legislative consultation.

**2) Strengthening of the EDPS' consultative role** - Article 42 of Regulation (EU) 2018/1725 has strengthened the consultative role of the EDPS by establishing a clear positive obligation for the European Commission to consult us on legislative proposals and other proposals with an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.

**3) Growing awareness of data protection issues** - There is a growing awareness of data protection issues amongst European Commission departments. In line with established practices, the European Commission is required to consult the EDPS in certain situations and is encouraged to consult us informally, according to Recital 60 of Regulation (EU) 2018/1725. This growing awareness is due to both the outreach we have undertaken, as well as the useful clarifications provided by the European Commission in its internal manuals of procedure, and the instructions of the Secretary-General regarding the consultation of the EDPS and the EDPB.





	2018	2019	2020	2021
Formal comments	13	3	19	76
Informal comments	33	16	13	28
Joint EDPS-EDPB Opinions	0	1	0	5
EDPS Opinions	7	6	8	12
EDPS own-initiative Opinions	1	1	2	0
Art. 57(1)(g)	2	2	2	1
Total	56	29	44	122

*Figure 13: Evolution of legislative consultations since 2018*

## 6.2.

# Key Opinions issued in 2021

We issue Opinions in response to mandatory requests by the European Commission, which is legally obliged to seek our guidance on any legislative proposal, draft implementing act or draft delegated act, as well as recommendations and proposals to the European Council in the context of international agreements, according to Article 42(1) of Regulation (EU) 2018/1725. Opinions are available in English, French and German on the EDPS website. Summaries of these Opinions are available in all official languages of the EU and are published in the Official Journal of the EU.

In 2021, a series of significant EDPS Opinions have been issued on three themes in particular: digital platforms, financial services and justice and home affairs.

### 6.2.1.

## Digital Platforms

### The Digital Services Act and the Digital Markets Act

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.

In our Opinion, we welcomed the proposal for a Digital Services Act that seeks to promote a transparent and safe online environment. We recommended additional measures to better protect individuals when it comes to content moderation, online targeted advertising and recommender 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 Act 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.



### 6.2.2.

## Financial Services

### 1. The Anti-Money Laundering legislative package

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.

### 2. The Proposal for a Regulation on Markets in Crypto-assets

We issued an [Opinion](#) on 24 June 2021 on the European Commission's Proposal to regulate the crypto-assets markets.

The proposed Regulation includes a series of obligations and requirements concerning the trading of electronic money tokens, rules on the authorisation and supervision of those issuing and/or providing electronic money tokens, and rules to protect individuals purchasing electronic money tokens. Overall, the Regulation seeks to prevent abuse in the crypto-assets markets.

We made a number of recommendations concerning this proposal, in particular about the responsibilities of those issuing crypto-assets.

As per the proposal, it is envisaged that issuers of crypto-assets may process the personal data of those purchasing crypto-assets by using various technologies and infrastructures, such as blockchain - a type of technology used in this case to record the purchasing and issuing of crypto-assets. Concerning the processing of individuals' personal data, issuers of crypto-assets may be considered [data controllers](#), since they decide for which purposes individuals' data may be processed and in what capacity, as well as the overall configuration of the crypto-asset project.

Given the type of personal data that may be processed and the infrastructure possibly used for this processing, we recommended that the issuers of crypto-assets - as possible data controllers - carry out a [Data Protection Impact Assessment](#) (DPIA). A DPIA would allow issuers of crypto-assets to evaluate the risks of all possible processing operations, and measures to mitigate such risks, as per the obligation set out in the [General Data Protection Regulation](#) (GDPR) applicable in the EU Member States.

In our concluding remarks, we suggested that issuers of crypto-assets explain in a transparent and simple way to individuals purchasing crypto-assets how their personal data may be processed.


### 6.2.3.

## The field of Justice and Home Affairs

### 1. Opinion on Proposed EU-UK Trade and Classified Information-Exchange Agreements

On 22 February 2021, we published our [Opinion](#) on two proposed agreements between the EU and the UK: the Trade and Cooperation Agreement (TCA) and an agreement on the security procedures for exchanging and protecting classified information.

Given the close cooperation that is expected to continue between the EU and the UK, we welcomed these two agreements. In particular, we noted that the TCA is based on respecting and safeguarding human rights and the parties' commitment to ensuring a high level of protection of personal data.



Nevertheless, the EDPS regretted that the TCA failed to faithfully take over the [EU's horizontal provisions for cross-border data flows and for personal data protection](#). Such provisions, which the European Commission has repeatedly stated as non-negotiable, allow the EU to include measures to facilitate cross-border data flows in trade agreements while preserving individuals' fundamental rights to data protection and privacy. Thus, in amending these horizontal provisions, the TCA creates legal uncertainty about the EU's position on the protection of personal data in the context of trade agreements and risks creating friction with the EU data protection legal framework.

## 2. Opinion on Schengen evaluations

On 27 July 2021, the EDPS published its [Opinion](#) on the European Commission's proposed Regulation establishing an evaluation and monitoring mechanism to verify whether the rights and obligations related to [Schengen](#) are applied (Schengen evaluations). The Schengen area includes most EU Member States and several non-EU countries, and enhances the freedom of movement for millions of individuals. EU Member States are responsible for upholding the rights and obligations related to Schengen, which include measures on border management, the Schengen visa, police cooperation and data protection. Its legal framework, the Schengen acquis, comprises various measures, including an evaluation and monitoring mechanism.

The European Commission's proposal, repealing [Regulation \(EU\) 1053/2013](#), has several objectives, such as streamlining the verification procedures of the Schengen evaluations to increase their effectiveness and efficiency. We acknowledged that the proposal seeks to strengthen EU Member States' involvement in the Schengen evaluations, as well as greater cooperation between the European institutions, bodies and agencies (EUIs) that are involved in the application of the rights and obligations related to Schengen.

We supported, in particular, the reform's goal to put in place measures ensuring that individuals' fundamental rights are protected when verifications occur.

Nevertheless, we recommended that the proposed Regulation clearly define the scope of the Schengen evaluations by drawing up a non-exhaustive list of relevant policy fields that would be subject to evaluation.

The reformed Schengen evaluations should also continue to provide for evaluations dedicated to data protection, carried out by data protection experts.

### 3. EDPS Opinion on Europol's mandate review

On 8 March 2021, we published an [Opinion](#) on the proposed amendments to the [Europol Regulation](#). These amendments aim, in part, to broaden the scope of [Europol's](#) mandate in response to changes in the security landscape and increasingly complex threats.

We assessed the necessity and proportionality of these proposed amendments, taking into account the importance of aligning the data protection rules for Europol with the data protection rules for other EUIs under Regulation (EU) 2018/1725.

In particular, the proposed exemptions related to the processing of large and complex datasets require further safeguards, so that the exemptions do not become the rule in practice. Effective personal data protection requires the situations and conditions in which Europol may rely on the proposed exemptions to be clearly defined in the Europol Regulation.

As the supervisory authority of Europol and other EUIs, we called for a full alignment of its powers with Regulation (EU) 2018/1725. When it comes to the protection of individuals' personal data, a stronger mandate of Europol must go hand in hand with oversight powers that are at least as strong and effective as for any other EUIs.



### 6.3.

## EDPS-EDPB Joint Opinions

According to Article 42(2) of Regulation (EU) 2018/1725, the European Commission may also consult the EDPB, in addition to the EDPS, on proposals of “particular importance” for personal data protection. In such cases, the EDPS and EDPB work collaboratively to issue a Joint Opinion.

In 2021, the EDPS and the EDPB have produced five Joint Opinions. Producing and delivering these Joint Opinions requires a great deal of collaboration and the sharing of expertise between all DPAs, including the EDPS. This collaboration and sharing of knowledge is essential, especially given the similarities between the GDPR and Regulation (EU) 2018/1725.

### 6.3.1.

## The Artificial Intelligence Act

With the EDPB, we adopted a [Joint Opinion](#) on 21 June 2021 on the European Commission’s Proposal for a Regulation laying down harmonised rules on artificial intelligence (AI).

We strongly welcomed the aim of addressing the use of AI systems within the European Union, including the use of AI systems by EUIs. At the same time, we expressed our concerns regarding the exclusion of international law enforcement cooperation from the scope of the Proposal.

We stressed the need to explicitly clarify that existing EU data protection legislation (the GDPR, Regulation (EU) 2018/1725 and the [Law Enforcement Directive](#)) applies to any processing of personal data falling under the scope of the draft AI Regulation.

Taking into account the extremely high risks posed by remote biometric identification of individuals in publicly accessible spaces, we called for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context.

Similarly, we recommended a ban on AI systems using biometrics to categorise individuals into clusters based on ethnicity, gender, political or sexual orientation, or other grounds on which discrimination is prohibited under [Article 21](#) of the EU Charter of Fundamental Rights.

Furthermore, we considered that the use of AI to infer emotions of an individual is highly undesirable and should be prohibited. It should only be allowed for very specified cases, such as some health purposes where the patient emotion recognition is important. The use of AI for any type of social scoring should also be prohibited.

### 6.3.2.

## The Digital Green Certificate

On 6 April 2021, together with the EDPB, we adopted a [Joint Opinion on the Proposals for a Digital Green Certificate](#). The Digital Green Certificate aims to facilitate the exercise of the right to free movement within the EU during the COVID-19 pandemic, by establishing a common framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, testing and recovery certificates.

With this Joint Opinion, we invited the co-legislators to ensure that the Digital Green Certificate is fully in line with EU personal data protection legislation. The data protection commissioners from all EU/EEA countries highlight the need to mitigate the risks to fundamental rights of EU citizens and residents that may result from issuing the Digital Green Certificate, including its possible unintended secondary uses.

The Joint Opinion underlined that the use of the Digital Green Certificate may not, in any way, result in direct or indirect discrimination of individuals, and must be fully in line with the fundamental principles of necessity, proportionality and effectiveness. Given the nature of the measures put forward by the Proposal, we considered that the introduction of the Digital Green Certificate should be accompanied by a comprehensive legal framework.



### 6.3.3.

## Standard Contractual Clauses

On 15 January 2021, we adopted Joint Opinions on two sets of contractual clauses (SCCs): a [Joint Opinion on SCCs between controllers and processors](#), which set out Controller-Processor SCCs, and a [Joint Opinion on SCCs for the transfer of personal data to third countries](#).

The Controller-Processor SCCs will have an EU-wide effect and aims to ensure full harmonisation and legal certainty across the EU when it comes to contracts between controllers and processors.

We welcomed the Controller-Processor SCCs as a single, strong and EU-wide accountability tool that will facilitate the compliance of controllers and processors with their obligations under the GDPR and Regulation (EU) 2018/1725.

Nevertheless, we requested several amendments in order to bring more clarity to the text and to ensure its practical usefulness in the day-to-day operations of controllers and processors. For example, it should be made clear to the parties involved when precisely they may rely on these SCCs. It should be emphasised that situations involving transfers outside the EU should not be excluded.

The draft SCCs for the transfer of personal data to third countries, under [Article 46\(2\)\(c\)](#) of the GDPR, will replace the existing SCCs for international transfers that were adopted under the previous Directive 95/46/EC ([Data Protection Directive](#)). These SCCs have been updated to take into account the GDPR's requirements, the "Schrems II" Judgement and to better reflect the widespread use of new and more complex data processing operations, which often involve multiple data importers and exporters.

Overall, in this Joint Opinion, we noted that the draft SCCs present a reinforced level of protection for individuals, but we believe that several provisions could be improved or clarified. The SCCs should ensure that the personal data of EU citizens is afforded an essentially equivalent level of protection when transfers to non-EU/EEA countries take place. Furthermore, the conditions under which SCCs may be used must be clear for organisations, and individuals should be provided with effective rights and remedies.

#### 6.3.4.

### The Data Governance Act

On 10 March 2021, we adopted with the EDPB a [Joint Opinion on the proposal for a Data Governance Act \(DGA\)](#). The DGA aims to foster the availability of data by increasing trust in data intermediaries (providers of data sharing services) and by strengthening data-sharing mechanisms across the EU. In particular, the DGA intends to promote the availability of public sector data for reuse, sharing of data amongst businesses and allowing personal data to be used with the help of a “personal data-sharing intermediary”. The DGA also seeks to enable the use of data for altruistic purposes.

We acknowledged the legitimate objective of the DGA to improve the conditions for data sharing in the internal market. At the same time, the protection of personal data is an essential and integral element for trust in the digital economy. With this Joint Opinion, we invited the co-legislators to ensure that the future DGA is fully in line with EU personal data protection legislation, thus fostering trust in the digital economy and upholding the level of protection provided by EU law under the supervision of the EU Member States’ DPAs.

#### 6.4.

### Key formal comments issued in 2021

Similar to our Opinions, our Formal Comments are issued in response to a request from the European Commission under Article 42(1) of Regulation 2018/1725 and address the data protection implications of legislative proposals. However, they are usually shorter and more technical, or only address certain aspects of a proposal. Our Formal Comments are published on our website in English, French and German.

In 2021, we issued 76 formal comments on various subjects, including a number related to Justice and Home Affairs and the European Health Union package.

#### 6.4.1.

### Formal Comments in Justice and Home Affairs

In May 2021, the EDPS issued five sets of Formal Comments on matters related to the functioning of [large-scale IT systems](#) in the field of Justice and Home Affairs. Large-scale IT systems are used to support EU policies on asylum, border management, policy cooperation and migration.


Our first set of [Formal Comments](#) addressed the requirements to be able to use audio and video to conduct an interview - if necessary - when individuals from non-EU countries apply for travel authorisation to EU Member States. Such requirements aim to ensure that the individuals interviewed have their privacy and personal data protected.

Our second set of [Formal Comments](#) focused on the cooperation procedure between the following large-scale IT systems in the event of a security incident:

- The future [Entry-Exit System](#) (EES);
- The [Visa Information System](#) (VIS);
- The [Schengen Information System](#) (SIS);
- The future [European Travel Information and Authorisation System](#) (ETIAS);
- The [European Criminal Records Information System](#) (ECRIS) for nationals from non-EU countries; and
- [EURODAC](#), a database including fingerprint data from asylum seekers.

Our third set of [Formal Comments](#) were on the European Search Portal (ESP), a centralised single-search interface that allows the searching of individuals' information across the following EU's large-scale IT systems: SIS, VIS, EURODAC, EES, ETIAS, ECRIS for nationals from non-EU countries. For the ESP to become operable, we recommended that [eu-LISA](#), the European Union Agency for the Operational Management of large-scale IT systems in the Area of Freedom, Security and Justice, in cooperation with the EU Member States, create a profile for each category of users that will need to have access to the search portal, based on the purpose of this access. These technical measures would ensure that individuals' personal data is sufficiently protected.

Our fourth set of [Formal Comments](#) concerned the same ESP, which will also be used to search data related to individuals or their travel documents in the



databases of [Europol](#), an EU body that actively cooperates with EU Member States' law enforcement authorities to combat serious international crime and terrorism, and [Interpol](#), the international criminal police organisation. In our Formal Comments, we addressed, in particular, the technical measures of the interoperability between the ESP, Europol and Interpol to ensure that individuals' personal data is sufficiently protected.

In our fifth set of [Formal Comments](#), we provided recommendations regarding the Multiple-Identity Detector (MID), one of the components that contributes to the interoperability of the EU's large-scale IT systems, facilitating therefore the search of individuals' personal data and their travel documents for example. The MID aims to prevent identity fraud by creating links between individuals' personal data located in the EU's different databases, for example SIS or ETIAS. Linking identities with the MID means that there are new and additional data processing operations involved. As such, linking data between the different databases should be strictly limited to the data necessary to verify an individual's identity.

#### 6.4.2.

### The European Health Union Package

On 18 March 2021, we issued Formal Comments on a package of three legislative proposals for a European Health Union. These proposals aimed to improve the protection, prevention, preparedness and response to human health hazards at the EU level. They include:

- the [Proposal](#) for a reinforced role of the [European Medicines Agency](#) (EMA) in crisis preparedness and management for medicinal products and medical devices;
- the [Proposal](#) on establishing a [European Centre for Disease Prevention and Control](#) (ECDC);
- the [Proposal](#) for a Regulation on serious cross-border threats to health.

In our three sets of Formal Comments, we welcomed the proposals' overarching aim to provide for a European approach to tackle cross-border health threats, building on the lessons learned from the COVID-19 pandemic. We supported a particular focus regarding the importance of coordination amongst European countries to protect people's health - both during a crisis and during normal times - when tackling underlying health conditions,

investing in strong health systems and training the healthcare workforce. Given the role that the EMA and the ECDC played during the COVID-19 pandemic, we took note of the positive steps envisaged to broaden their tasks to achieve the objectives set out in the proposal.

6.5.

## Case Law Digest on Transfers of Personal Data

We publish [Case Law Digests](#) to highlight and explain complex data protection issues using relevant case law in this area.

Case Law Digests are aimed at individuals who have an advanced understanding of data protection issues. Our readership therefore includes academics, people working at relevant EUIs, and other stakeholders working in the field of data protection.

To this end, our Case Law Digests aim to help with particular challenges or provide some answers to questions on data protection issues that may come up in our stakeholders' day-to-day work.

Each Case Law Digest we produce is [published](#) on the EDPS website.

6.5.1.

### Transfers of personal data to non-EU/EEA countries

In June 2021, we published a [Case Law Digest](#) focusing on transfers of personal data outside the EU/EEA, as interpreted by the [Court of Justice of the European Union](#) (CJEU). With this Case Law Digest, the EDPS reiterated the overarching principle of the "EU law of transfers", according to which the continuity of protection of personal data, and therefore the protection of fundamental rights and freedoms of the individual, is maintained - even when someone's personal data "travels" outside the EU/EEA.

To help the reader navigate this complex topic and the extensive judgements of the CJEU, from "[Lindqvist](#)" in 2003 to "[Schrems II](#)" in

2020, we curated nine questions addressing key issues concerning transfers of personal data, including:

- what does an adequate level of protection mean when transfers of personal data to non-EU/EEA countries occur?
- when, why and subject to which conditions are SCCs considered valid by the CJEU as a tool for transfers of personal data?
- what are the powers available to EU/EEA DPAs when transferring personal data to non-EU/EEA countries?


Read our Case Law Digest, [here](#).



The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting small, semi-transparent blue dots. These dots and lines are scattered across the page, creating a sense of a digital or interconnected space. The lines and dots are more concentrated in some areas, forming a web-like structure, while other areas are sparser.

## **CHAPTER SEVEN**

# **The EDPS as a member of the EDPB**



The European Data Protection Board (EDPB) is an EU body established under the [General Data Protection Regulation](#) that promotes cooperation between Data Protection Authorities (DPAs) to ensure the consistent application of data protection rules across the EU. The EDPS is both a member of the EDPB and the provider of an independent Secretariat that offers administrative and logistic support, performs analytical work and contributes to the EDPB's tasks. A [Memorandum of Understanding](#) lays down the terms of cooperation between the EDPS and the EDPB.

## 7.1.

# Enforcement, support and coordination

### 7.1.1.

## The Support Pool of Experts

Consistent and efficient enforcement of the GDPR remains a priority. Resources available for the DPAs are sometimes insufficient and there are some discrepancies caused by the different legal frameworks and national procedural laws. In response to these practical constraints, we believe that solidarity and reinforced cooperation with the EDPB and other related actors are key. To accompany DPAs in their work and to assist in the carrying out of investigations and enforcement activities of significant common interest, we proposed the establishment of a Support Pool of Experts ([SPE](#)) comprising both EDPB experts and external experts within the EDPB.

Together with the EDPB Secretariat and other EDPB members, we developed terms of reference as a basis for establishing the SPE, as outlined in the [EDPB Strategy 2021-2023](#).

In December 2021, the European Data Protection Board adopted a project plan for the Support Pool of Experts. The SPE will be deployed to provide expertise (e.g. assisting analysis, investigative reports and performance findings) and enhance cooperation to support investigations and enforcement activities. This initiative aims to provide support to DPAs on complex and resource-demanding cases in a genuine expression of European solidarity and burden sharing.



### 7.1.2.

## The EDPB's first ever coordinated action

On 20 October 2020, the EDPB set up a [Coordinated Enforcement Framework](#) (CEF), which provides a structure for coordinating recurring annual activities by national data protection authorities (DPAs). The framework focuses on a pre-defined topic and allows DPAs to pursue this topic using the agreed methodology. Following the proposal made by the EDPS, the EDPB decided that the first action would concern the use of cloud-based services by public sector bodies.

Public sector bodies have a duty to lead by example, including when it comes to outsourcing. Moreover, any improvements of compliance in services provided to the public sector are also likely to lead to improvements in services provided to the private sector. Most, if not all, public sector bodies in the EEA face similar difficulties in trying to obtain Information and Communications Technology (ICT) products and services that comply with EU data protection laws. Coordinated guidance and action by DPAs are necessary to bring about meaningful change in the market. Appropriate safeguards, such as technical and organisational measures, should be put in place when processing this data to minimise risks for the privacy of individuals.

On 13 October 2021, the EDPB decided to launch its [first coordinated action](#), in which we intend to participate by focusing on compliance of EUIs' use of cloud services with Regulation (EU) 2018/1725, which lays out the data protection obligations for EUIs when they process personal data and develop new policies. Given the similarities between the GDPR, applicable to most public and private entities in the EU Member States, and Regulation (EU) 2018/1725, applicable to EUIs, it is important to ensure the same level of protection regarding the use of cloud-based services by both EU Member States' entities and the EUIs.

### 7.1.3.

## The active participation of the EDPS in the EDPB


The EDPS has substantial involvement with the EDPB, which is illustrated in particular by our active participation in EDPB meetings and with the work we carry out when acting as lead or co-rapporteur (i.e. lead or co-case handler) for specific EDPB Guidelines, Recommendations, Opinions or other documents.

As a member of the EDPB, we have made substantial contributions to EDPB documents covering a wide range of topics, such as transfers of personal data, as well as the dispute resolution and urgency procedures. Some of these examples are detailed below.

### 1. EDPB Opinions on adequacy decisions

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.

In the Opinions detailed below, the members of the EDPB, which includes the EDPS, assess different elements with the aim to provide the European Commission with an opinion for the assessment of the adequacy of the level of protection of the non-EU/EEA country concerned. Examples of these elements include the type of processing involved; the purpose of processing; the type of data; how long it will be processed for and how it will be stored.



The key objective of the EDPB in Opinions 14/2021 and 15/2021 on the UK adequacy decisions, and Opinion 32/2021 on the Republic of Korea's adequacy decision was to respond to the European Commission's draft adequacy decisions based on the draft decisions themselves and an analysis of relevant documentation. In all three Opinions, the EDPB identified many areas of convergence between the EU frameworks and the non-EU/EEA frameworks. Beyond these areas of essential, equivalence, however, the EDPB identified some key challenges, outlined below.

**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 Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive**

- The Law Enforcement Directive (LED) lays down the specific rules about the processing of personal data by competent authorities for the purposes of the prevention; investigation; detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against the prevention of threats to public security. In its Recommendations, the EDPB established the core data protection principles that have to be present in a non-EU/EEA country or an international organisation's legal framework to ensure an essential equivalence with the EU framework within the scope of the LED.

### **EDPB Recommendations 01/2020 on measures that supplement data transfer tools**

The Court of Justice of the European Union (CJEU) clarified that individuals whose data is transferred to non-EU/EEA countries should be afforded a level of protection that is essentially equivalent to that guaranteed within the EU/EEA. This means that data exporters should carry out a transfer impact assessment to make sure that such level of protection is guaranteed and identify appropriate measures supplementing their transfer instrument, where needed. To help with this task, the EDPB [directed](#) (in its recommendations 01/2020 published in June 2021) data exporters to take the following steps:

- Know your transfers by being aware of where the personal data you transfer is going;
- Verify the transfer tool your transfer relies on;
- Assess if there is anything in the law and/or practices in force of the non-EU/EEA that could impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer;
- Identify and adopt any necessary supplementary measures;
- Take any formal procedural steps that the adoption of the supplementary measure may require; and
- Re-evaluate at appropriate intervals your analysis of the level of protection afforded to the personal data you transfer to third countries.



## 2. EDPB work on dispute resolution and urgency procedures

The EDPS provided a substantive contribution to the drafting of the guidelines and decisions in relation to Article 65 of the GDPR on dispute resolution by the EDPB, and Article 66 of the GDPR on urgency procedure. [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.

- **EDPB Guidelines 09/2020 on relevant and reasoned objection**
  - This document offers guidance on what is considered a relevant and reasoned objection under the GDPR. For an objection to be “relevant”, there must be a direct connection between the objection and the substance of the draft decision at issue. For an objection to be “reasoned”, it needs to include clarifications and arguments as to why an amendment of the decision is proposed.
- **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.

- **EDPB first urgent binding decision** - The EDPB adopted its first urgent binding decision under Article 66(2) of the GDPR following a request made by the Hamburg DPA within the framework of the urgency procedure under Article 66 GDPR. The Hamburg DPA came to the conclusion that Facebook Ireland Ltd (Facebook IE) was already processing the data of WhatsApp users residing in Germany for its own purposes. In some cases this processing was done following the notification by WhatsApp Ireland Ltd to German users of its new Terms of Service and Privacy Policy, and the extension of the deadline for users to provide consent by 15 May 2021. Through provisional measures, the Hamburg DPA prohibited Facebook IE from processing personal data of WhatsApp users residing in Germany, which is transmitted from WhatsApp IE to Facebook IE, for three months. The EDPB decided that the conditions to prove the existence of an infringement to the GDPR and the urgency to adopt final measures were not met, hence stating that the Irish DPA did not need to adopt final measures against Facebook IE.

An abstract graphic on a dark blue background featuring a network of light blue dots connected by thin lines, creating a web-like pattern. The dots and lines are more concentrated on the left side and fade out towards the right.

## **CHAPTER EIGHT**

# **International cooperation**



As per the Foresight pillar of our [Strategy 2020- 2024](#), the EDPS aims to be alert to and aware of the new trends in technology and data protection, and to cooperate with data protection authorities from the EU and beyond. In 2021, we continued to dedicate substantial time in promoting cross-border dialogue and data protection convergence within the EU and beyond. Despite the pandemic-related challenges, we have actively participated in European and international fora, and continued to exchange best practices and information with international organisations and interlocutors outside Europe.

### 8.1.

## The 43rd Global Privacy Assembly

We took part in the 43rd Global Privacy Assembly, hosted by the National Institute for Transparency, Access to Information and Protection of Personal Data ([INAI](#)) in Mexico, between 18 and 21 October 2021. The Supervisor, the Director and our EDPS colleagues participated in various online panels.

The [Global Privacy Assembly \(GPA\)](#), previously named International Conference of Data Protection and Privacy Commissioners, is an international forum with more than 130 data protection and privacy authorities from across the globe that gather to connect and share their perspectives on the developments in data protection and key elements of their international cooperation. During the 43rd edition of the GPA, a number of resolutions were adopted concerning:

- the Assembly's Strategic Direction;
- data sharing for the public good;
- children's digital rights;
- governments' access to data; and
- the future of the Global Privacy Assembly.

To find out more about the 43rd Global Privacy Assembly, its reports and resolutions, please consult [this webpage](#) on the EDPS website.



## 8.2.

# Council of Europe

### 8.2.1.

## The activities of the Consultative Committee to the Convention 108


The Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data on 28 January 1981. The Convention, known as [Convention 108](#), is the first binding international instrument in the data protection sphere. Any country may sign up to the Convention, including countries that are not members of the Council of Europe. To this date, 55 countries are now party to the Convention and its additional Protocol regarding Data Protection Authorities and transborder data flows.

On 18 May 2018, the Protocol amending the Convention was adopted. It reaffirms the essential principles enshrined in the original Convention text and integrates new data protection safeguards. The modernised Convention, known as Convention 108+, was opened for signature on 10 October 2018.

We participated as an observer in the Council of Europe's expert groups on data protection, such as the Consultative Committee (T-PD) of Convention 108. Our role involves ensuring a high standard of data protection and compatibility with EU data protection standards. As of March 2019, we also represent the GPA in the T-PD.

In recent months, the EDPS followed in particular and more specifically the following activities of the Council of Europe:

- the [Evaluation and review mechanism under Convention 108+](#);
- the [Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns](#);
- the [Guidelines on facial recognition \(T-PD\(2020\)03rev4\)](#);
- a new [Opinion on the draft second additional Protocol to the Budapest Convention](#);

- 
- a [Report on “Digital solutions to fight COVID-19”](#);
  - the [development of contractual clauses in the context of transborder data flows](#).

#### 8.2.2.

### The Council of Europe’s work on artificial intelligence

The Council of Europe Ad Hoc Committee on Artificial Intelligence ([CAHAI](#)) was established in 2019 to examine the feasibility and potential elements of a legal framework for the development, design and application of artificial intelligence technologies, based on the Council of Europe’s standards in the field of human rights, democracy and the rule of law.

In line with its mandate, the CAHAI prepared two important documents: a feasibility study and a document with the potential elements of a binding legal framework for the development, design and application of artificial intelligence. The former document concluded that the appropriate legal framework should consist of a combination of binding and non-binding legal instruments. The latter document identified a number of concrete elements for a future convention on AI, including fundamental principles, risk classification of AI systems, “red lines” for AI applications creating unacceptable risk, democratic governance, supervision, and other key aspects. In addition, the CAHAI developed a model for a human rights, democracy, and rule of law impact assessment (HUDERIA) for AI systems.

We participated in the activities of the CAHAI together with the European Commission and the EU’s Fundamental Rights Agency. EDPS representatives contributed, in particular, to the work of the two main expert groups of CAHAI - the Policy Development Group (CAHAI-PDG) and the Legal Framework Group (CAHAI-LFG).

### 8.3.

## The Computers, Privacy and Data Protection Conference


Each year, the Computers Privacy and Data Protection Conference (CPDP) brings together academics, lawyers, practitioners, policymakers, computer scientists and civil society to exchange ideas about data protection and information technology.

As a CPDP side event, we organised a webinar on 25 January 2021 titled: “Data for the public good: Building a healthier digital future”, with the aim to reflect on the impact of the legal and technical measures taken in response to COVID-19.

During the event, experts from various fields addressed three main themes, namely public health; digital transformation; and the impact on fundamental rights, such as freedom of movement, data protection and non-discrimination.

The first panel of experts discussed the EU’s and EU Member States’ initial approach to the pandemic, the role that data has played in monitoring its evolution in Europe and in the facilitation of risk management, but also the challenges linked to the increased reliance on and use of digital technologies.

The second panel of experts focused on the way data and technology may be used in the future, particularly from a health perspective. Experts highlighted the importance of data to create new opportunities; access to health data for primary use and also secondary use was referred to as being essential, but still complex to achieve in practice. At the same time, special attention must be paid to ensure that this data is only used for the public or the common good and not misused for other gains than societal ones.



Since then, we continue to engage in productive discussions like these to inform our work and to ensure that the fundamental rights of data protection and privacy are embedded in each solution envisaged to overcome any obstacle to an effective and efficient use of data for the public good.

Throughout the CPDP conference, the Supervisor reiterated that privacy, like any fundamental right, is nothing without solidarity, because an individual's right is the right of an entire society.

#### 8.4.

### Cooperation with International organisations

Generating and fostering global partnerships in the field of data protection is a priority for the EDPS.

One of the ways in which we do this is by co-organising a yearly workshop dedicated to data protection within [international organisations](#).

The workshop is a forum for the exchange of experiences and views on the most pressing issues in data protection faced by international organisations all over the world. The size and relevance of this event has been growing since its first edition in 2005. This confirms the need for a platform for international organisations to engage, share best practices and discuss unsolved dilemmas, and also demonstrates the increasing awareness of how important it is to ensure strong safeguards to protect individuals' personal data.

The 2020 remote workshop of data protection within International Organisations demonstrated a strong demand on the size of international organisations to have an in-depth discussion on practical tools to facilitate international transfers.

As a follow-up, in 2021, the EDPS led the activities of a taskforce on international transfers to international organisations with a view to develop concrete solutions to frame transfers to international organisations. This work is still ongoing and the next in-person edition of the workshop with international organisations will take place in May 2022. Unfortunately, no workshop was held in 2021 due to the COVID-19 pandemic.

An abstract graphic on a dark blue background featuring a network of light blue dots connected by thin lines, creating a web-like structure. The dots and lines are more concentrated on the left side and fade out towards the right.

## **CHAPTER NINE**

# **Cooperation with Civil Society**

In 2021, we continued to cooperate with [civil society organisations](#) that advocate for privacy and data protection rights.

On 25 January 2021, we organised with the [EDRi](#) network, which works to defend digital rights, a Civil Society Summit, titled "Big tech: from private platforms to public infrastructures" in the context of the [Privacy Camp 2021](#).

The EDPS-Civil Society Summit considered that the intensely centralised nature of the digital economy presents fundamental challenges for our times and future generations. As a matter of fact, a limited number of big tech companies exercise significant control over the internet as a network, whereby the sharing of information, freedom of expression and individuals' choices are increasingly under the influence of corporate interests. In addition, public authority is being outsourced to private companies, as holders of essential infrastructures, to safeguard and regulate our digital lives.

Corporations that started as search engines and social media platforms are now exercising significant influence in healthcare, education and public administration. Others have become indispensable to a huge number of business users, or to enable work processes. Some other big tech companies dictate the terms of our social interactions, and occupy the public space of freedom of expression and influence political opinions. This power grabbing has further intensified the power and "indispensability" of big tech companies as platforms, but also as service providers, decision-makers, and gatekeepers.

In the 2021 edition of the EDPS Civil Society Summit, we explored, in a dynamic exchange with civil society, the wider consequences of the data intensive business models of dominant tech companies. In particular, speakers outlined the consequences for fundamental rights, and broader societal concerns.

As such, the following issues, amongst others, were addressed during the EDPS-Civil Society Summit:

- Who is in the end paying the costs of the societal shift of changing control of public infrastructures?
- On whose terms is such a shift taking place?
- How does this impact people and their fundamental rights?
- What are the requirements of data governance models to address this?



The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting various-sized dots of the same color. The dots and lines are scattered across the page, creating a sense of interconnectedness and digital structure. The lines form a web-like pattern, with some dots acting as central hubs and others as peripheral nodes.

## **CHAPTER TEN**

# **Transparency and access to documents**



As an EUI and according to our Rules of Procedure, the EDPS is subject to [Regulation \(EC\) No 1049/2001](#) (Regulation (EC) 1049/2001) regarding public access to European Parliament, Council and Commission documents. Regulation (EC) 1049/2001 governs the fundamental right of EU citizens and residents to have access to documents held by the EU institutions. This Regulation lays down the general principles, limits, rules and procedures to the public access of documents held by EUIs. At the EDPS, the person responsible for handling these requests is a designated Transparency Officer. The appointed officer collaborates with the relevant staff members to respond timely and appropriately to the requests.


The EDPS adopted a new Case Manual on Public Access to Documents on 30 October 2021 and in parallel, the transparency officer started streamlining the internal processing of access to document requests. In addition, the EDPS enabled a Public Documents Registry on 6 December 2021, according to the requirements of Regulation (EC) 1049/2001. In 2021, the EDPS received 27 initial access to documents requests. In three of these cases, the EDPS also received a confirmatory application. In all cases where documents could be identified, the requested documents were either fully or partially disclosed.

All other transparency and communication actions are available on the EDPS website, including access to the EDPS accounts on Twitter, LinkedIn, YouTube and the EDPS RSS feed. We remain fully committed to increasing the transparency and accountability of our work and aim to update our website, and our public documents registry with relevant documents and information on a regular basis.

The background of the slide is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting numerous small, semi-transparent blue dots. These dots and lines are scattered across the entire frame, creating a sense of interconnectedness and digital structure. The lines vary in length and orientation, forming a web-like pattern that is denser in some areas and sparser in others.

## **CHAPTER ELEVEN**

# **The EDPS' communication activities**



Public interest in and engagement with data protection and the work of Data Protection Authorities (DPAs) continues to grow, 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 Sector (I&C Sector) aims to, therefore, ensure that EDPS activities and messages reach the relevant audiences at the right time.

The role of the I&C Sector, reinforced in the [EDPS Strategy 2020-2024](#), is to explain and promote the work of the EDPS. This commits 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' day-to-day work in clear language and via appropriate communication tools.

#### 11.1.

### The EDPS' corporate image

In 2020 and early 2021, we developed a new visual identity to mark the EDPS' new mandate and modernise its style. 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. Our visual identity has been adapted to all our publications: press releases, Opinions, Formal Comments, Speeches, videos, to ensure that the general public and relevant actors in the data protection field can easily recognise who we are.

The visual identity first materialised with the launch of the EDPS [corporate brochure](#) and [corporate video](#) on 20 January 2021.

The [brochure](#), titled "Shaping a Safer Digital Future", presents the EDPS to the public by providing an insight into our role, tasks and responsibilities as the EU's data independent DPA, as well as giving a snapshot of the EDPS 2020-2024 strategy. The brochure was published in all official languages of the EU because data protection concerns all of us.

The [corporate video](#) is an extension of the EDPS corporate brochure. It provides an overview of how European institutions, bodies and agencies (EUIs) may process individuals' personal data and in what contexts, and how the EDPS ensures that this is done in compliance with [Regulation \(EU\) 2018/1725](#), the data protection regulation applicable to EU institutions.

11.2.

## Our social media channels

The EDPS has a well-established presence on three social media channels, which we are able to use to reach a global audience easily and quickly.

11.2.1.

### Twitter

[@EU\\_EDPS](#) has been a valuable social media tool to promote the EDPS' presence at a variety of events and to feature the core messages and purpose of our work.

Our latest tweets are always available to view on the EDPS homepage.

11.2.2.

### LinkedIn

[LinkedIn](#) allows us to communicate in a more detailed way with data protection specialists and other actors in the field of data protection. In 2021, our LinkedIn channel popularity has consistently grown with increasing engagement, reaching 50,000 followers.

We pursued our Social Media campaigns, examples of which are detailed below.

- **#InCaseYouMissedIt:** As we continue to welcome new followers to our ever-growing social media community, we run the #InCaseYouMissedIt campaign twice a year to raise awareness of less high-profile topics, inform data protection officers (DPOs), controllers and processors of their obligations by promoting our factsheets and guidelines.

- In 2021, we continued our campaign **#CelebratingEU** to inform our audience about the role and cooperation we have with national DPAs.

### 11.2.3.

## YouTube

**YouTube:** In 2021, we used this platform to raise awareness about certain aspects of data protection. Videos on our YouTube channel are usually published alongside factsheets on the same topic, this includes, for example, the topic of personal data breaches. This medium allows us to provide important information in a quick, clear and concise way. To increase the visibility and accessibility of our work, our videos are routinely published in English, French and German. These videos, like the one on personal data breaches, are mostly targeted to Data Protection Officers (DPOs) of the EUIs with the aim to inform them on how to apply certain aspects of EU data protection law. When preparing these videos, we also keep in mind that they may be of interest to the DPOs within the EU Member States, given the similarities between Regulation (EU) 2018/1725 and the GDPR.

Our YouTube channel is also a way for us to retransmit important events that we have organised or participated in, such as the [IPEN webinars](#), or [the AI stakeholder summit 2021](#). Our viewers therefore have the opportunity to watch or re-watch some important discussions and exchanges the EDPS had with relevant actors in the field of data protection. These efforts also contribute to making our work more accessible and transparent, which are two important values of the EDPS, as set out in our strategy.

The YouTube channel also enables us to deliver more personal messages, and to elaborate in more detail on our work, plans and projects, especially since much of our work has been carried out remotely over the last two years. For example, we produced a [video](#) with the EDPS' Technology and Privacy colleagues for the reception of our TechDispatch award in November 2021. We also prepared a video in which the Supervisor details and explains his plans for the EDPS' upcoming conference in June 2022.

### 11.3.

## EDPS Website

The EDPS' main website, managed by the I&C sector, is continuously improved by adding new features and enhancing its design, in response to our visitors' feedback and needs.

On a more technical level, we completed the migration of our website to Drupal 8, which we started in 2020, and we have now started the migration of our website to Drupal 9, which was started at the end of 2021. These improvements both facilitate the users' overall experience in the way they consume our content, but also facilitates our internal use of the website when it comes to publishing EDPS content.

In cooperation with the EDPS' Data Protection Officer and the EDPS' Transparency Officer, we also designed the following webpages:

- a new register for the Public Access to Documents ([see chapter 10](#));
- a new records register of data processing activities;
- an updated version of our EDPS cookie banner ([see chapter 13](#)).

In addition, we also introduced a new webpage titled, [TechSonar](#).

While most of the EDPS' activities can be found on our main website, we also created, and continue to develop other dedicated websites when necessary for specific purposes and projects:

- the creation of a mini-website with the EDPB to mark the annual EU Open Day as an alternative to the traditional in-person event which could not be held due to the COVID-19 pandemic;
- the development of a dedicated website for the EDPS' upcoming Conference in 2022 on the future of data protection.

11.4.

## Publications

11.4.1.

### Factsheets

In 2021, we published four factsheets, some of which are accompanied by a video.

This year's factsheets provide an overview of:

- the [EDPS enforcement powers](#);
- [personal data breaches](#): "Personal data breaches in a nutshell";
- [data protection audits](#): "What to expect when we inspect-Data protection audits explained"; and
- [cybersecurity](#): "Stop, Think, Look".

Most of our factsheets are available in English, French and German. In just four or five pages, our readers - from the data protection officers of EUIs and of the EU Member States to individuals interested in data protection - are provided with an overview and explanation of a particular aspect of EU data protection law and other resources to further explore the topic addressed in these factsheets.

11.4.2.

### EDPS newsletters

The [EDPS Newsletter](#) continues to grow in popularity as an accessible and user-friendly communication tool on all digital devices and platforms. The newsletter proves to be an essential communication tool allowing us to respond to our audience's differing interests and levels of expertise concerning data protection matters.

In 2021, we published seven newsletters to keep our audience up to date with EDPS activities in an approachable, condensed and informative way.

Each issue of the EDPS newsletter in 2021 covered approximately 15 topics, ranging from the EDPS' technology monitoring activities, our latest Opinions and Formal Comments, the EDPS' Supervision and Enforcement actions, the EDPS' work as a member of the EDPB, events that the EDPS organised or participated in, to name a few examples.

#### 11.4.3.

### EDPS blog

The [EDPS blog](#) is a platform through which the European Data Protection Supervisor, Wojciech Wiewiórowski, the Director and, more recently, the EDPS' Heads of Units, are able to communicate on a more personal level about their thoughts, opinions and activities, as well as the work of the EDPS in general. The EDPS blog is also a space for the EDPB and EDPS trainees to describe their projects, ideas and traineeship experience.

Now active for over five years, the EDPS blog has established itself as an essential EDPS communication tool. The blog can be easily found on the homepage of our main website where a short extract from the most recent blogpost is always displayed.

In 2021, the EDPS published 11 blogposts on an array of subject matters.

This medium has proved to be useful, not just in 2021, but also in recent years, to provide more details on:

- what is discussed during the bi-annual meetings of the network of DPOs, given the importance of the DPOs' contribution to the compliance with data protection laws within the EUIs;
- our technological monitoring efforts;
- the events that we have organised; and
- an insight into the EDPS-EDPB traineeship.

Blogposts that we published in 2021 also focused on the reporting the events organised by the EDPS. This included IPEN webinars, CPDP side events and the EDPS-EDPB trainees' conference. We also used this platform to explain in detail new initiatives launched by the EDPS in 2021, such as TechSonar.





11.5.

## Virtual and in-person events

11.5.1.

### Europe Day

Europe Day is a day celebrating peace and unity in Europe. It is celebrated on 9 May every year. As the independent DPA in charge of supervising the way EUIs process your personal data, it is a chance for us to celebrate the achievements made in the field of data protection and privacy.

On this occasion, with the [EDPB](#), we created an interactive webpage to help you learn more about what both of our organisations do on a daily basis. By scrolling down the EDPS - EDPB webpage, readers were able to consult both of our organisations' videos and brochures to find out more about data protection, how their personal data is processed when using social media or search engines for example, and about their privacy rights.

11.5.2.

### Celebrating Data Protection Day

To mark Data Protection Day, together with the EDPB, we took part in the Computers, Privacy and Data Protection Conference ([CPDP](#)) and organised CPDP side events. CPDP brings together academics, lawyers, practitioners, policymakers, computer scientists and civil society to exchange ideas about data protection and information technology. Notably, we organised an online CPDP side event, titled, "[Data for the public good: Building a healthier digital future](#)". The aim was to assess the impact of measures taken in response to the COVID-19 pandemic and identify ways in which data can be used to be better prepared for the next one. Finally, the EDPS and the EDPB organised an online booth for visitors to virtually join and exchange information.

### 11.5.3.

## Trainees' conference and podcast

Twice a year, the EDPS and EDPB welcome [trainees](#) for a period of five months, from October to February, and from March to July. It is the custom that trainees work on a specific project to mark the end of their traineeship, which they organise from scratch with the support of the EDPS members of staff, including the I&C sector, when necessary. In February 2021, the EDPS and EDPB trainees launched a podcast series, and in July 2021, the trainees organised an online conference.


### 1. EDPS- EDPB trainees' first podcast

In February 2021, the EDPS and EDPB trainees launched a new [podcast](#) titled Democratic Societies in the Digital Age. This is the first ever podcast series that the trainees have produced in an effort to try something new and unique. The three-part series brings together experts from wide-ranging professional backgrounds and nationalities to answer the following question: Do all roads lead to datocracy? Along the way, our guest speakers shared their thoughts on a number of pertinent topics, such as mass surveillance and facial recognition technologies, online manipulation and dark patterns, emerging technologies and future challenges.

The [first episode](#) provides information on the role of the data protection framework and the correlation between private and public surveillance actors. The [second episode](#) focuses on the issues of online manipulation and dark patterns. The guest speakers discussed the level of deceptiveness used online to trick users into purchasing items, for example. The final [episode](#) touches on emerging technologies and future challenges that may have an impact on data protection.

### 2. Trainees' conference on biometric surveillance

Following the EDPS and EDPB's [Joint Opinion on the European Commission's recent proposal for an AI Regulation](#), the trainees planned a conference titled: "[An Orwellian Premonition: a discussion on the perils of biometric surveillance](#)", held on 14 July 2021. With a focus on biometric surveillance, the EDPS and EDPB trainees explored possible implications stemming from the European Commission's Proposal.



Distinguished speakers from wide-ranging areas of expertise - lawyers, university professors and civil liberty activists - were invited to share their views on the technical, legal and ethical elements of biometric surveillance. The conference highlighted concerns about the different ways biometric data could possibly be abused if biometric surveillance were legalised. Panellists also widened the scope of the conference by including an international perspective on this issue.

#### 11.5.4.

### International events


Throughout 2021, we were involved in the planning and communicating of both international events organised by the EDPS and international events in which the EDPS participated. These events included:

- **EDPS-Civil Society Summit** (26 January 2021) - The EDPS-Civil society summit is an annual meeting between the EDPS and civil society organisations organised to discuss the state of data protection and privacy in the EU.
- **The annual Computers, Privacy and Data Protection Conference (CPDP)** (26 January 2021) - CPDP brings together academics, lawyers, practitioners, policymakers, computer scientists and civil society to exchange ideas about data protection and information technology.
- **Global Privacy Assembly** (20-21 October 2021) - An international forum with more than 130 data protection and privacy authorities. Discussions at the forum ranged from the future of privacy and technology to individuals' digital and privacy rights in a hyper-connected society.

#### 11.5.5.

### Study visits

We have hosted an increasing number of study visits at the EDPS in the last few years. As the profile of data protection has increased, so has interest in our work. Although we would like to host every group that expresses an interest in what we do, our high workload and the limited resources available to host these visits has forced us to limit study visits



to specialist groups of 10 or more individuals, such as university students at post-graduate level.

Nevertheless, study visits comprise an important part of our communications strategy, allowing us to raise awareness about data protection and our work.

Due to the national and EU rules related to the COVID-19 pandemic, we had to forego all in-person visits, but instead offered the option of an online presentation with a Q&A session.

We had six study visit requests in 2021.

## 11.6.

# External relations

## 11.6.1.

# Press releases

The EDPS frequently interacts with the media through [press releases](#), interviews and press events. We issue press releases on significant data protection developments and activities that the EDPS has contributed to, such as the outcome of investigations, Opinions and reports. All of our press releases are published on the EDPS and on the EU Newsroom websites. They are also distributed to our network of journalists and other interested parties.

We published 16 press releases in 2021 covering several different areas related to data protection, digital privacy and new technological developments. Some examples of this include:

- the EDPS' follow-up actions to the "Schrems II" ruling compliance strategy and investigations;
- developments related to Artificial Intelligence;
- several joint press releases with the EDPB; and
- Opinions on matters related to transfers of personal data in the context of trade agreements, for the purpose of monitoring criminal activities.

### 11.6.2.

## Media relations

The topics that garnered most attention in 2021 are detailed below.


- **Artificial intelligence:** In particular our EDPS-EDPB Press Release and Joint Opinion, published in June 2021, on the European Commission's Proposal for an Artificial Intelligence Act, in which we call for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces.
- **Our Joint Press Releases and Joint Opinions with the EDPB** more generally. These touched on a variety of topics, such as the Data Governance Act (DGA), on [contractual clauses](#) in the context of transfers of personal data, and on the EU legislators' Proposals for a [Digital Green Certificate](#).
- **The EDPS' follow-up work to "Schrems II" investigations and on transfers of personal data in general**, especially the two EDPS investigations launched as part of the Supervisor's [strategy for EU institutions to comply with the "Schrems II" ruling](#), so that ongoing and future international transfers are carried out according to EU data protection law.
- **The EDPS' upcoming [Conference in June 2022](#)** on the future of data protection and the effective enforcement in the digital world. The announcement of the EDPS Conference in November 2021 attracted lots of media attention, mainly on how to lead the discussion on the world's best practices when it comes to enforcement action and cooperation, while also exploring alternative models of enforcement for the digital future.

These topics prompted all sorts of media enquiries, such as requests for follow-up interviews with the Supervisor.

### 11.6.3.

## Responding to requests from the public

In 2021, we recorded an increase in public requests for information. While we still receive many requests related to matters which do not fall under the EDPS' competences, mainly because they are of national



scope and not EU related. We have also received a growing number of requests in recent months that have been more complex and submitted by individuals who are keen to learn more about the work that we do, the powers that we have and their rights when it comes to the processing of their personal data. We reply to all requests with the relevant information for the enquiry. This involves referring individuals to the relevant service if their request falls outside our competence or providing them with the appropriate information to answer their query. Requests are mainly addressed to us in English, French or German, and we always reply in the language used by the requester, as long as the request is formulated in one of the EU's official language.

11.7.

## Employer branding

Any organisation is only as good as its people; the ability of an organisation to deliver depends on the quality of its staff. Therefore, it is essential for the EDPS, as a growing EUI, to not only attract highly qualified individuals, but also to keep them motivated.

With this approach in mind, we adopted our Employer Branding Strategy, which aims to increase our visibility as an employer, by strengthening the reputation of the EDPS as a top career destination and attracting new talents in 2021. This initiative involves various communication activities foreseen for 2021-2024. Some examples of the communication activities we carried out and will pursue in the coming years include:

- a LinkedIn campaign known as #EDPScareers, which presents the EDPS as an employer and showcases our organisation's culture, values and principles.
- regular updates of the [EDPS' careers page](#) of our website.
- a revamp of the EDPS' Vacancy Notices to align them with the new visual identity and present our vacancies in a more candidate-centred way.
- a Staff Ambassadors Club, launched in late 2021. Staff Ambassadors will take part in a campaign planned for the beginning of 2022, which aims to promote the EDPS as a workplace.

While the I&C sector has taken the lead on these activities, we work in close collaboration with the HRBA Unit of the EDPS.

11.8.

## Preparing the EDPS Conference

Following the Supervisor's announcement of his conference, titled "The future of data protection: effective enforcement in the digital world", on 16 and 17 June 2022 in Brussels, Belgium, the I&C sector, along with members of the EDPS conference task force, is involved in the preparatory work of the conference.

So far, our work for the conference has consisted of the production of a video in which the EDPS explains the conference, the design of the explanatory leaflet, the preparation of a dedicated conference [website](#) available in English, French and German, and the choice of venue. More work is envisaged in the first six months of 2022.

The aim of this conference is to bring together stakeholders from the digital regulatory sphere to reflect on and discuss enforcement models pertaining to data protection, competition, digital markets and services and, artificial intelligence. We expect that this conference will encourage a constructive discussion on the different approaches to data protection enforcement. The conference also aims to facilitate the sharing of best practices in this area.

To find out more, read the [EDPS' Conference Leaflet](#) and watch the [video address](#), both of which are available on our website.

The EDPS' Communication activities	
Followers on YouTube	2438 followers
Followers on Twitter	25826 followers
Number of tweets	637
Followers on LinkedIn	49575 followers
Number of study visits	6
Number of information requests requests for info from public where EDPS is competent	53
+ requests for info from public where EDPS is not directly competent	164
Number of press requests - Requests for interview from press	38
Requests for info from press	39
Newsletter subscribers	6234
Number of press releases	16
Number of blogposts	11

*Figure 14: Statistics on Communication Activities*






The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract geometric pattern consisting of numerous thin, light blue lines that connect small, semi-transparent blue dots. These dots and lines are scattered across the page, creating a network-like or molecular structure that is more dense in some areas and sparser in others. The overall effect is a modern, technological, and interconnected aesthetic.

## CHAPTER TWELVE

# Human Resources, Budget and Administration



Throughout 2021, the EDPS' Human Resources, Budget and Administration Unit (HRBA) has provided support to the Management and Operational teams at the EDPS. The aim is to ensure that they have sufficient financial, human and administrative resources and tools to achieve the goals set out in the [EDPS Strategy 2020-2024](#).

### 12.1.

## A safe return to the office

During 2021, the HRBA unit continued to closely monitor the evolution of the ongoing pandemic and aligned its administrative decisions with the measures put in place by the Belgian authorities, as well as the measures adopted by other EUIs. In July 2021, the HRBA unit devised an internal strategy for our gradual return to the office, which was presented to all EDPS members of staff and discussed with the staff committee, before it was endorsed by the management team.

Our return to the office plan was built on a phased approach, similar to other EUIs. We implemented different phases over the course of the pandemic. Each phase had specific working arrangements, and health and safety rules. All our EDPS colleagues were regularly informed about any step forward or backward in the light of the evolving epidemiological situation. For example, phases ranged from:

- **Phase 0** - Complete lockdown.
- **Phase 1** - Cautious relaxing of measures related to COVID-19; teleworking remains the norm.
- **Phase 2** - Progressive relaxing of measures related to COVID-19; regular presence at the office.
- **Phase 3** - Towards a "new normal" combination of telework with increased office presence.

As part of the plan, in September 2021, the HRBA unit ran a survey on the current vaccination status of our colleagues and their satisfaction with health and safety measures in the office. The findings highlighted an overall vaccination rate of at least 80% amongst our colleagues and most of them considered the current health and safety measures in place to be sufficient. The survey results allowed the EDPS management to justify progressing to phase 2 of the "return to work" strategy.

Due to a resurgence of COVID-19, the HRBA unit introduced several COVID-19-related measures in December 2021. Measures included an impact assessment, an executive decision and a protocol for the European Parliament's security service in charge of the buildings' entrance surveillance. The measures, which were based on the [EDPS guidance](#) on our "return to work" strategy issued to all EUIs in August 2021, envisaged the use of manual and visual checks of COVID-19 certificates as the least intrusive for an individual's privacy, thus abiding by the principle of minimisation.

## 12.2.

### Well-being at work

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

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

We believe that staff who report higher levels of positivity, comfort and happiness at work are more likely to learn more effectively, be more creative, have better work-relationships, be more pro-social in their behaviour, feel more satisfied in their jobs and perform better. Therefore, encouraging well-being at work is of vital importance at the EDPS.

To this end, HRBA appointed a Well-being Coordinator to ensure that internal HR processes are in line with EDPS staff's well-being, and that colleagues have the knowledge and tools necessary to facilitate a high level of well-being at work, and whenever possible outside of work.

The Well-being Coordinator role is normally held by an HR representative, as an approach focused on well-being immensely benefits recruitment and training, career planning, performance and talent management, engagement and recognition, leaving and retirement.

The Well-being Coordinator applies the following principles:

- encouraging an enjoyable working environment;
- giving staff a voice;
- ensuring that the EDPS values are demonstrated;
- treating every person as a human being who matters.

The Well-being Coordinator, together with the EDPS' internal coach, or the EDPS Staff Committee, managed to organise well-being activities in 2021, even if some of these activities had to be postponed or cancelled due to the pandemic. Activities that could go ahead include:

- **Team walks** – Our internal coach assisted each EDPS unit and sector in launching the team-walks initiative, which allowed colleagues in the same unit or sector to connect, and take stock of their experiences working together and to decide on the team's future path, in an informal setting.
- **Office leisure activities** – Our colleagues were encouraged to organise various leisure activities in small groups. The activities could include organising a book club, playing board games and solving puzzles, food tasting group or a language round table. These leisure activities will happen until our return to the office, when the time is right.

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



12.3.

## Recruiting data protection experts

The EDPS has grown rapidly in 2021 and will continue to do so in 2022. To ensure that we have the personnel and expertise to carry out the tasks assigned to us as the data protection authority of EUIs, there is a need to hire more data protection experts. EUIs can select candidates for permanent contracts through open competitions. Applicants who pass a competition are placed on a reserve list from which the relevant organisations recruit as and when they need them.

In response to the EDPS' needs, we are organising, with the support of the European Personnel Selection Office ([EPSO](#)), a new administrator (AD) specialist competition for individuals who will hold an administrator grade of AD 6. This means that candidates need a few years of relevant experience to be eligible for this competition as it is a specialised role. The aim of this competition is to have a reserve list of data protection experts, from which we will be able to recruit as from 2022. This reserve list will enable us to satisfy our new recruitment needs, as well as cover our usual staff turnover for the next years.

We have volunteered to be the pilot for a new fast-track model of competition and this time, other EUIs are participating. We are hopeful that this competition will result in establishing a list of 76 successful laureates. The notice for the competition was published in September 2021 and the main stages of this competition will take place during the first semester of 2022. We aim to publish the reserve list during the second half of 2022.

12.4.

## Employer branding

The HRBA Sector helped the I&C sector of the EDPS in building and delivering the EDPS' Employer branding strategy to promote the EDPS as a top career destination.

Amongst the various initiatives carried out in 2021, and to be pursued in 2022 ([see 11.7](#)), the HRBA unit contributed to the revamping of our vacancy notices, with the view to making them more attractive, clearer

and more candidate-oriented in line with the EDPS' culture. We also started a LinkedIn Network of EDPS trainees, with the aim of creating a professional community where former and current trainees can exchange relevant information.

## 12.5.

# Adapting our working conditions


The changes in our working environment caused by the pandemic and the full-time teleworking regime called for a deep reflection on the adaptation of our working conditions. For this reflection, we considered factors including working time, hybrid working and telework from abroad. The HRBA unit began this reflection and will propose new rules, which will be discussed and agreed upon by our staff committee. The aim is to adopt these rules by mid - 2022.

HRBA has made proposals to amend the reimbursement of public transportation set up to provide our EDPS colleagues with greater flexibility regarding transportation reimbursements. After a pilot phase, we will conduct an assessment and make changes if needed. In addition, we supported our staff during the teleworking period by offering the possibility to buy an office chair and a screen that are partially reimbursed.

## 12.5.1.

# Going paperless for some administrative procedures

We have modernised and simplified our appraisal procedure by introducing it in our HR management tool, Sysper, a platform allowing the management of HR resources. Sysper allows both employees and the employer of EUIs to consult their records, such as their personal file or appraisals. To modernise and simplify our appraisal procedure, we improved the process for managers, staff and the HR team, especially in the context of remote working. This also contributes to our efforts to become a paperless administration.



In addition, we have initiated the process to automate the management of the probationary periods of officials and contract agents. Some technical issues have delayed the setup of this process until the beginning of 2022.

#### 12.5.2.

### Coaching and activities for staff

In 2021, we continued to provide internal coaching and other activities for EDPS and EDPB staff, to help improve individual job performance and relationships at work. Coaching focuses on developing strengths, making changes and helping find specific solutions to professional challenges.

Our internal coach conducted over 25 individual sessions in full confidentiality in 2021. Our coach also provided team coaching, accompanying teams in improving their working relations or setting priorities and goals in their work. Due to the pandemic, many of these team and coaching events took the form of walks. Various activities took place to help our colleagues get to know each other better during these walks.

Throughout 2021, the management team also benefited from two sessions of team coaching.

#### Other activities

- **Online workshops** - We organised online workshops for all the EDPS and EDPB teams (Units and Sectors) on finding work-life balance and building resilience. During these workshops, we raised awareness on stress patterns, burnout, how to alleviate stress and improve resilience. Participants also shared the measures they adopt to manage their stress. We also discussed strategies on how staff can support each other and build their resilience as a team.
- **Co-development** – In March 2021, a pilot co-development project was established for heads of activities and deputy heads of units of the EDPS and EDPB. Professional co-development is a type of group coaching in which participants learn from each other and consolidate their professional practice together. It involves a structured consultation exercise, covering real-life issues encountered by the participants. During the sessions, participants take turns to act as “clients” and “consultants”. The aim of this exercise is to identify any

issues or problems our colleagues may be facing in their role and find solutions to help improve their understanding and capacity to act in these situations. We intend to continue these sessions in 2022.

- **Virtual coffees** - We also organised random virtual coffees for staff to join on a voluntary basis. Our colleagues were put into breakout sessions in pairs on a random basis for 10 minutes, during which they were invited to share opinions on different questions. This gave staff the opportunity to meet up with colleagues they might not see often.

## 12.6.

# Budget

### 12.6.1.

## Budget execution

Similar to 2020's budget implementation, the budgetary execution for 2021 was once again substantially impacted by the COVID-19 pandemic. The movement of our staff and individuals within Belgium was severely restricted. These restrictions affected several different areas of our budget implementation such as mission expenses, travel costs, organisation of events and participation at events. In addition, the rapid increase of COVID-19 cases in Europe towards the end of 2021 also led to the cancellation of many planned events, which directly impacted our budget implementation for the year.

The committed appropriations amounted to 16.761.285€ out of an overall budget of 19.463.193€. Therefore, in 2021, the EDPS budget execution was 86,12%, which represents an improvement compared to the execution of 2020 of 72,33%.



### 12.6.2.

## Budget preparation and budget monitoring

Bluebell, a system created by the [European Research Council's Executive Agency](#) for budget management, was fully effective in 2021. This system enabled us to become more efficient during the budget preparation as it improves the budget monitoring. It is the main resource of communication between, on one hand, the operational services of the EDPS (i.e. Units and Sectors) implementing the Administrative Budget and, on the other hand, the Finance Sector. Finally, the system saves a historical archive of all versions of the budget (requested and allocated), supporting documents, as well as activities and comments done by the different actors during the budgeting and forecasting process.

In 2021, two operational units of the EDPB and the EDPS used Bluebell as pilot units. Their feedback was positive; consequently the EDPS - as a whole - will use this tool for the budget preparation and the periodic budget reviews, starting on 1 February 2022.

The budget structure evolved slightly in 2021. It was mainly modified to better reflect the actual needs of the Secretariat of the EDPB.


### 12.6.3.

## Finance

As a result of the EDPS' growth and the new budget structure of the organisation, the number of budgetary commitments to cover expenses in the year 2021 increased substantially. Indeed, between 2020 and 2021, the number of budgetary commitments increased by 26.72%, from 131 commitments to 167 commitments.

Given that the EDPS' activities were expanded and diversified, the most noticeable increase concerns provisional budgetary commitments, with a growth of 57%.

Another factor that explains these increases is the rollout of the budget management tool, Bluebell (see 12.6.2).



In addition, and as a consequence of the increase of the number of budgetary commitments, the payment amounts increased also significantly by 17,50% (from 14.150.455,00€ in 2020 to 16.625.500€ in 2021).

12.7.

## Public Procurement

The HRBA Unit's public procurement procedures are usually dictated by both the EDPS' and the EDPB's working programs and plans for the upcoming year. This may include the need to outsource certain activities, for example particular events, conferences, and other projects.

In this respect, part of HRBA's role is to support both institutions in public procurement procedures, by ensuring that these are conducted smoothly and that they comply with the budgetary principles laid down in the Financial Regulation for EUIs. More specifically, the HRBA Unit concentrated its efforts on making sure that the external contractors collaborating with the EDPS and the EDPB meet the necessary moral and ethical standards expected from all EUIs; uphold the highest professional conduct throughout the contract; and respect the environmental, social and human rights defended by the EU. Throughout the entire process of a public procurement procedure, the HRBA Unit prioritises an open, fair, transparent selection and competition process. The aim is to make these procedures more accessible to a wider range of talents, irrespective of a contractor's background. Indeed, we believe that an environment that favours healthy competition, fosters a qualitative collaboration between the EDPS and/or the EDPB and the contractor(s) in question.

The projects that involved call for tenders, and the subsequent establishment of framework contracts, in 2021 included:

- EDPS initiatives related to transfers of personal data to non-EU/EEA countries.
- EDPS' and EDPB's communication activities.
- the EDPS' upcoming conference to be held on 16-17 June 2022, titled: ["The Future of Data Protection: Effective Enforcement in the Digital World"](#).

12.8.

## Learning and development

In 2021, the HRBA Unit continued to offer training courses via EU-LEARN to its staff. EU-LEARN is a platform for all employees of EUIs to sign up to training courses that contribute to enhancing and developing new skills related to their position or organisation. The platform includes training courses on a wide range of topics, from perfecting language skills, interpersonal skills and courses related to EUIs' core business activity, such as data protection. Managers could take management-focused courses with the European School of Administration. As with previous years, external trainings were also offered to our staff.

HRBA continued with the "HRBA teasers" in 2021. This initiative was launched in 2019 and has proven to be appreciated by colleagues.

The "teasers" are short presentations covering procedures, tools and topics of interest for new colleagues. They aim to help newcomers better understand the role and function of HRBA within the EDPS, which, in turn, improves everyday workplace proceedings. The teasers cover topics including internal IT systems and processes, such as SYSPER2, a platform managing administrative documents linked to employees, and MIPs, an inter-institutional platform to manage expenses in the case of professional/business trips and missions. The teasers also include a Q&A for newcomers and the EU learning and development basic information regarding practical modalities and information about the EU-LEARN platform. HRBA aims to increase the number of teasers in 2022.

HRBA has continued in 2021 to invite all new staff members to an online Learning and Development presentation during "welcome days". HRBA provided newcomers at the EDPS with information about and links to online training sessions, as well as the opportunity to raise specific questions. HRBA published a Frequently Asked Questions section on the EDPS intranet to specifically address questions on procedures and work during the COVID-19 pandemic.

12.9.

## The European House of Data Protection

Following the moving of the European Ombudsman at the end of October 2021, the EDPS and the EDPB became the sole occupants of its current premises in Brussels. This paved the way for us to start creating and establishing our premises as “The European House of Data Protection”, with the aim of becoming the EU’s Brussels-based hub for privacy and data protection. This project started in 2021 and will continue throughout 2022.

To adapt the building’s facilities for this purpose, the HRBA Unit organised in November 2021 the refurbishment of the three floors previously occupied by the European Ombudsman. Following this, over 100 members of staff of the EDPS and EDPB moved offices to occupy the newly-available space. In addition, the HRBA Unit coordinated the transformation of common areas of various floors of the premises into larger meeting rooms with portable teleconferencing systems; a dedicated room for lunchtime and coffee breaks, known as the Cloud within our organisation; an IT Lab; a library/study space; and a wellbeing room. Furthermore, a new press studio is being installed, which is to be finalised in 2022.

The work carried out to transform our premises into the European House of Data Protection was carried out in close cooperation with the relevant services of the European Parliament. This was also an opportunity for HRBA to continue building solid working relationships with other EUIs throughout 2021, with the use of administrative agreements, Memoranda of Understanding, and Service Level Agreements to ensure the effective and efficient running of the EDPS.

The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting small, semi-transparent blue dots. These dots and lines are scattered across the page, creating a sense of a digital or data network. The lines and dots are more concentrated in the upper left and lower right areas, with some sparse connections in the center.

## **CHAPTER THIRTEEN**

# **The EDPS' Data Protection Officer**

The focus of the [office of the Data Protection Officer \(DPO\)](#) at the EDPS in 2021 was to enhance the EDPS' data protection compliance, while always keeping the role and mission of the EDPS in mind.

Considering the EDPS' role as the data protection authority (DPA) of the European institutions, bodies and agencies (EUIs), as well as the high level of in-house expertise in the field, the DPO office, together with the services in charge of personal data processing, continued to lead by example by raising and upholding the highest standards of data protection throughout 2021. Moreover, as per the core action pillar of our [EDPS Strategy 2020-2024](#), the EDPS continued to support EUIs to continue to lead by example in safeguarding digital rights and responsible data processing.

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



13.1.

## Accountability

With a resolution to strengthen compliance, the DPO office put accountability into practice in a number of ways in 2021.

13.1.1.

### Monitoring the application of data protection rules

We constantly monitored the practical application of data protection rules and procedures in light of the legal provisions and case law.

13.1.2.

### Consolidating the EDPS' register of processing activities

We consolidated the [EDPS' register of personal data processing activities](#) with new and updated records and improved its layout to increase its accessibility.

13.1.3.

### Updating EDPS data protection notices

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

2021, we also regularly updated our data protection notices, such as in the context of EDPS events, webinars, videos, newsletter subscriptions.

#### 13.1.4.

### Making sure that services used by the EDPS are data protection compliant

We continued the process of scrutinising the services used by the EDPS in order to clarify the data protection responsibilities of all contracting parties and adapting, where appropriate, contractual clauses. For example, when the EDPS uses external contractors for media services, event planning, communication tools. This work will continue in 2022.

#### 13.1.5.

### Assessing data protection risks


We assessed the risks to the fundamental rights and freedoms of individuals of new and ongoing processing activities and carried out a Data Protection Impact Assessment regarding the processing of personal data in the context of the COVID-19 pandemic.

#### 13.1.6.

### Finding privacy and data protection friendly alternatives

We explored and analysed privacy and data protection friendly alternatives to limit reliance on services that involve transfers of personal data outside the EU and EEA. This includes our work on the use of ICT tools and a platform for online cooperation. This work started in 2021, and will be pursued in 2022.





### 13.1.7.

## Addressing requests from the EDPS as the EUIs' data protection authority

The DPO office also addressed requests made by the EDPS as the data protection authority of EUIs.

Like other EUIs, the EDPS replied to the survey on processing operations related to COVID-19 by providing information on new processing operations that have been determined by this context, including processing activities related to IT tools and solutions put in place, or enhanced, for working remotely.

The EDPS also provided the requested information and follow-up actions and information in the context of the remote audit under [Article 25](#) of Regulation (EU) 2018/1725 concerning restrictions of individuals' data protection rights. More specifically, the EDPS provided information on its [Internal Rules](#); information on the restrictions the EDPS applied; as well as information on recommendations put in place in the EDPS' draft Internal Rules. The audit was closed with no further recommendations.

### 13.2.

## Advising the EDPS

Throughout 2021, the DPO office continued to advise services in charge of personal data processing on a wide variety of subject matters.

In particular, the DPO office advised on the data protection compliance of new services considered to be used by the EDPS, for example in the fields of human resources, information security and communication. In many cases, a number of safeguards were put in place to ensure data protection compliance, including specific contractual terms tailored to the relevant circumstances. The DPO office continued to advise and work closely with services in charge of processing personal data related to COVID-19 in order to ensure this compliance; topics included manual contact tracing and building access.

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

### 13.3.

## Enquires and complaints

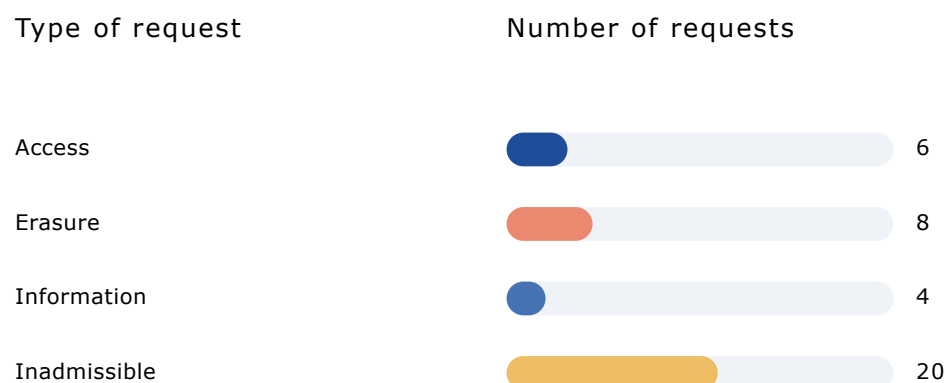
The number of enquiries, complaints and requests from individuals exercising their data protection rights received by the EDPS in 2021 increased in comparison to previous years.

The DPO office processed six access requests in 2021. An access request gives individuals the right to request a copy of their personal data that is being processed. These requests are often referred to as “data subject access requests” or “access requests”.

We also processed eight erasure requests, four information requests and twenty inadmissible requests. In certain cases, individuals exercised more than one data protection right, such as access and erasure requests.

Individuals may lodge a complaint with the EDPS, as a controller, if they believe their data protection rights have been infringed by the EDPS when processing their personal data, for instances such as:

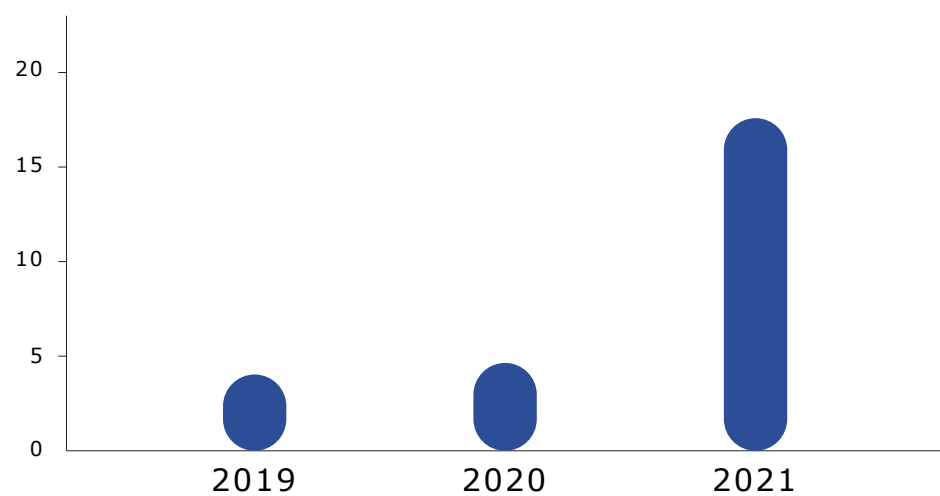
- excessive amounts of personal data being collected;
- personal data being shared with third parties without appropriate legal basis.



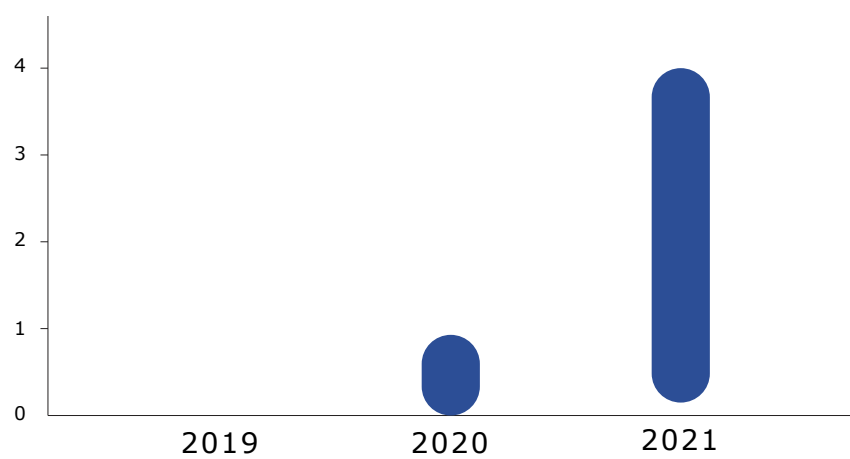
*Figure 15: Type of requests processed by the DPO of the EDPS in 2021*

Access to personal data was provided to the individual in one case, while in the other cases it was concluded that no personal data was processed. In all cases of erasure requests, the EDPS informed the applicants that it does not process their personal data.

During 2021, the EDPS received four complaints: two from EDPS staff and two from citizens. The complaints concerned unauthorised disclosure of personal data, processing without a legal basis and information provided to individuals. In one particular case, the complaint concerned the EDPS' cookie banner and the possibility to withdraw consent. After the EDPS' reply, the applicant confirmed that the issue was linked to the browser settings.



*Figure 16: Evolution of data subject requests since 2019*



*Figure 17: Evolution of complaints since 2019*



13.4.

## Raising awareness about data protection

The DPO office delivered a number of training sessions in 2021. The training session for new colleagues incorporates a module on data protection, which is regularly updated to take into account the latest developments in the field, including the most recent EDPS internal rules and procedures. Given the specificity of the EDPS, which as a rule recruits data protection specialists, particular attention is paid to tailor the content to the audience. As a result, presentations tend to focus more on internal rules and procedures, rather than general data protection concepts.

In order to raise awareness on data protection, we also organised an artistic competition for Data Protection Day 2021, which gave the opportunity to EDPS staff to employ both their expertise in data protection and their unique artistic talents. This competition was appreciated by our EDPS colleagues, as there was a variety of fascinating entries, for example poems, paintings and recipes. This competition is one of the ways to reinforce collegiality between the DPO and EDPS staff, and to raise awareness of data protection and discuss data protection in a unique manner.

13.5.

## Cooperation

The DPO office continued its collaboration with the DPOs of other EUIs, allowing for the valuable exchange of expertise and best practices in various formats, such as regular meetings and working groups on specific topics, which gather together DPOs and other experts. In addition, we participated in the biannual meetings with the network of DPOs in June and December 2021. The DPO office also participated in the regular meetings organised by the DPOs' network of the European Data Protection Board, made up of DPOs of national DPAs.

In order to foster cooperation and communication between the EDPS, as a DPA, and the EUIs' DPOs, a number of EDPS-DPOs roundtables were

organised. These roundtables provide a forum to discuss the application of data protection rules, possible solutions to ensure that individuals' data is adequately protected according to the EU's values and principles. In view of the EDPS-DPO meetings, the DPO participated in the DPO "support group" meetings organised by the EDPS.


Various topical subject matters were discussed, including the challenges of processing personal data in times of COVID-19; the use of video conference tools and its challenges; international transfers; as well as fostering cooperation between the EUIs' DPOs and the EDPS.



The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting small, semi-transparent blue dots. These dots and lines are scattered across the page, creating a sense of a global or digital network. The lines vary in length and orientation, forming a web-like structure.

## **ANNEX A**

# **Legal framework**



The European Data Protection Supervisor was established by [Regulation \(EC\) No 45/2001](#) of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The Regulation was based on Article 286 of the EC Treaty, now replaced by Article 16 of the [Treaty on the Functioning of the European Union](#) (TFEU). The Regulation also laid down appropriate rules for the institutions and bodies in line with the then existing EU legislation on data protection. It entered into force in 2001. A revised version of the Regulation, [Regulation \(EU\) No 2018/1725](#), entered into force on 11 December 2018.

Since the entry into force of the Lisbon Treaty on 1 December 2009, Article 16 TFEU must be considered as the legal basis for the EDPS. Article 16 underlines the importance of the protection of personal data in a more general way. Both Article 16 TFEU and Article 8 of the [EU Charter of Fundamental Rights](#) establish that compliance with data protection rules should be subject to control by an independent authority. At EU level, this authority is the EDPS.

Other relevant EU acts on data protection are:

- [Directive 95/46/EC](#), which was replaced by Regulation 2016/679, the General Data Protection Regulation ([GDPR](#)), on 25 May 2018. The GDPR lays down a general framework for data protection law in the Member States;
- [Directive 2002/58/EC on privacy and electronic communications](#) (as amended by [Directive 2009/136](#));
- [Directive on data protection in the police and justice sectors](#).

A new Regulation on privacy and electronic communications (ePrivacy) is currently under negotiation.

## **Background**

Article 8 of the [European Convention for the Protection of Human Rights and Fundamental Freedoms](#) provides for a right to respect for private and family life, subject to restrictions allowed only under certain conditions. However, in 1981 it was considered necessary to adopt a separate convention on data protection, in order to develop a positive and structural approach to the protection of fundamental rights and



freedoms which may be affected by the processing of personal data in a modern society. The convention, also known as Convention 108, has been ratified by more than 40 Member States of the Council of Europe, including all EU Member States. Convention 108 will be amended by its Protocol (CETS No 223) upon its entry into force.

Directive 95/46/EC, which was the predecessor to the GDPR, was based on the principles of Convention 108, but specified and developed them in many ways. It aimed to provide a high level of protection and a free flow of personal data in the EU. When the Commission made the proposal for this directive in the early 1990s, it stated that Community institutions and bodies should be covered by similar legal safeguards, thus enabling them to take part in a free flow of personal data, subject to equivalent rules of protection. However, until the adoption of Article 286 TEC, a legal basis for such an arrangement was lacking.

On 6 April 2016, the EU agreed to a major reform of its data protection framework, adopting the GDPR to replace the old Directive. The GDPR is an essential step forward in strengthening citizens' fundamental rights in the digital age. It focuses on reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards.

In addition to this, the GDPR increases the territorial scope of the EU's data protection rules, introduces administrative fines, strengthens the conditions for consent and gives people more control over their personal data, in particular making it easier to access.

The Treaty of Lisbon enhances the protection of fundamental rights in different ways. Respect for private and family life and protection of personal data are treated as separate fundamental rights in Articles 7 and 8 of the Charter. This is legally binding, both for the institutions and bodies, and for the EU Member States when they apply Union law. Data protection is also dealt with as a horizontal subject in Article 16 TFEU. This clearly indicates that data protection is regarded as a basic ingredient of good governance. Independent supervision is an essential element of this protection.

## **Regulation (EU) No 2018/1725**

According to Article 2(1), this Regulation applies to the processing of personal data by all Union institutions and bodies as of 11 December 2018. However, it only became applicable to the processing of personal data by Eurojust from 12 December 2019 and it does not apply to the processing of operational personal data by Europol and the European Public Prosecutor's Office, nor to the processing of personal data as part of activities referred to in Articles 42(1), 43 and 44 TEU, such as activities carried out within the framework of the common security and defence policy. In addition, only Article 3 and Chapter IX of the Regulation apply to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities of judicial cooperation in criminal matters or police cooperation.

The definitions and the substance of the Regulation closely follow the approach of the GDPR. It could be said that Regulation (EC) No 2018/1725 is the implementation of the GDPR at EU institution level. The structure of Regulation (EU) 2018/1725 should be understood as equivalent to the structure of the GDPR and whenever its provisions follow the GDPR they should be interpreted homogeneously. This means that the Regulation deals with general principles like fair and lawful processing, proportionality and compatible use, consent, including special conditions for children, special categories of sensitive data, as well as transparency, information and access to personal data and rights of the data subject. It addresses the obligations of controllers, joint controllers and processors, supervision, enforcement, remedies, liabilities and penalties. A specific section deals with the protection of personal data and privacy in the context of electronic communications. This section is the implementation for EU institutions and bodies of the Directive 2002/58/EC on privacy and electronic communications.

Regulation 45/2001 introduced the obligation for EU institutions and bodies to appoint at least one person as [data protection officer](#) (DPO) and Regulation (EU) 2018/1725 reaffirms this. These officers are tasked with ensuring the internal application of the provisions of the Regulation, including the proper notification of processing operations, in an independent manner. All institutions and most bodies now have these officers, and in some cases have done for many years. These officers are often in a better position to advise or to intervene at an early stage and to help to develop good practice. Since the DPO has the formal duty to

cooperate with the EDPS, this is a very important and highly appreciated network to work with and develop further.

### **Tasks and powers of the EDPS**

The tasks and powers of the EDPS are clearly described in Chapter VI and Articles 52, 57 and 58 of Regulation (EU) 2018/1725, both in general and in specific terms. Article 52 of Regulation (EU) 2018/1725 lays down the general mission of the EDPS — to ensure that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, with respect to the processing of personal data, are respected by EU institutions and bodies. Moreover, it sets out some broad lines for specific elements of this mission. These general responsibilities are developed in Articles 57 and 58 of Regulation (EU) 2018/1725 with a detailed list of tasks and powers. Among its tasks and powers, the EDPS provides the European Data Protection Board's (EDPB) secretariat, is a member of the EDPB, and participates in its activities. As such, and in accordance to Article 75 of the General Data Protection Regulation, a [Memorandum of Understanding](#) outlines the cooperation of the EDPS and EDPB.

This presentation of responsibilities, duties and powers follows a very similar pattern to those of the national supervisory bodies. These include hearing and investigating complaints, conducting other inquiries, informing controllers and data subjects and carrying out prior checks when processing operations present specific risks. The Regulation gives the EDPS the power to obtain access to relevant information and relevant premises, where this is necessary for inquiries. The EDPS can also impose sanctions, which now include administrative fines, and refer a case to the EU Court of Justice.

Some tasks are of a special nature. The task of advising the Commission and other EU institutions about new legislation — highlighted in Article 28(2) of Regulation 45/2001 and Article 42 of Regulation (EU) 2018/1725 by a formal obligation for the Commission to consult the EDPS when it adopts a legislative proposal relating to the protection of personal data — also relates to draft directives and other measures that are designed to apply at national level or to be implemented in national law. This is a strategic task that allows the EDPS to look at privacy implications at an early stage and to discuss any possible alternatives, including in areas that used to be part of the former third pillar (police and judicial

cooperation in criminal matters). Monitoring relevant developments which may have an impact on the protection of personal data and intervening in cases before the Court of Justice are also important tasks. In addition, pursuant to Article 42(2) of Regulation (EU) 2018/1725, the European Commission may consult the European Data Protection Board (EDPB), established to advise the European Commission and to develop harmonised policies under the GDPR, on proposals which are of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. In such cases, the EDPB and the EDPS coordinate their work with a view to issuing a joint opinion.

The duty to cooperate with national supervisory authorities and supervisory bodies in the former third pillar is also of strategic importance. Cooperation with supervisory bodies in the former third pillar allows the EDPS to observe developments in that context and to contribute to a more coherent and consistent framework for the protection of personal data, regardless of the pillar or the specific context involved. Under the previous legal framework, there was no single coherent model for coordinated supervision. Article 62 of Regulation (EU) 2018/1725 now allows for the implementation of one single model for coordinated supervision of large-scale information systems and of Union bodies, offices or agencies by the EDPS and national supervisory authorities.



## **ANNEX B**

# **Extract from Regulation (EU) 2018/1725**

#### **Article 41 - Information and consultation**

1. The Union institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures and internal rules relating to the processing of personal data by a Union institution or body, whether alone or jointly with others.
2. The Union institutions and bodies shall consult the European Data Protection Supervisor when drawing up the internal rules referred to in Article 25.

#### **Article 42 - Legislative consultation**

1. The Commission shall, following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the European Data Protection Supervisor where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.
2. Where an act referred to in paragraph 1 is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission may also consult the European Data Protection Board. In such cases the European Data Protection Supervisor and the European Data Protection Board shall coordinate their work with a view to issuing a joint opinion.
3. The advice referred to in paragraphs 1 and 2 shall be provided in writing within a period of up to eight weeks of receipt of the request for consultation referred to in paragraphs 1 and 2. In urgent cases, or if otherwise appropriate, the Commission may shorten the deadline.
4. This Article shall not apply where the Commission is required, pursuant to Regulation (EU) 2016/679, to consult the European Data Protection Board.



## **Article 52 - European Data Protection Supervisor**

1. The European Data Protection Supervisor is hereby established.
2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies.
3. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and of any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends, the European Data Protection Supervisor shall fulfil the tasks set out in Article 57 and exercise the powers granted in Article 58.
4. Regulation (EC) No 1049/2001 shall apply to documents held by the European Data Protection Supervisor. The European Data Protection Supervisor shall adopt detailed rules for applying Regulation (EC) No 1049/2001 with regard to those documents.

## **Article 57 - Tasks**


1. Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall:
  - a. monitor and enforce the application of this Regulation by Union institutions and bodies, with the exception of the processing of personal data by the Court of Justice acting in its judicial capacity;
  - b. promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
  - c. promote the awareness of controllers and processors of their obligations under this Regulation;
  - d. upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the national supervisory authorities to that end;

- e. handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 67, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
- f. conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
- g. advise, on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;
- h. monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;
- i. adopt standard contractual clauses referred to in Article 29(8) and in point (c) of Article 48(2);
- j. establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39(4);
- k. participate in the activities of the European Data Protection Board;
- l. provide the secretariat for the European Data Protection Board, in accordance with Article 75 of Regulation (EU) 2016/679;
- m. give advice on the processing referred to in Article 40(2);
- n. authorise contractual clauses and provisions referred to in Article 48(3);
- o. keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2);
- p. fulfil any other tasks related to the protection of personal data; and
- q. establish his or her Rules of Procedure.

2. The European Data Protection Supervisor shall facilitate the submission of complaints referred to in point (e) of paragraph 1 by a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of the European Data Protection





Supervisor shall be free of charge for the data subject.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the European Data Protection Supervisor may refuse to act on the request. The European Data Protection Supervisor shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

#### **Article 58 — Powers**

1. The European Data Protection Supervisor shall have the following investigative powers:

- a. to order the controller and the processor to provide any information it requires for the performance of his or her tasks;
- b. to carry out investigations in the form of data protection audits;
- c. to notify the controller or the processor of an alleged infringement of this Regulation;
- d. to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of his or her tasks;
- e. to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union law.
- f. The European Data Protection Supervisor shall have the following corrective powers:
- g. to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- h. to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- i. to refer matters to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;
- j. to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- k. to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate,

in a specified manner and within a specified period;

- l. to order the controller to communicate a personal data breach to the data subject;
  - m. to impose a temporary or definitive limitation including a ban on processing;
  - n. to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;
  - o. to impose an administrative fine pursuant to Article 66 in the case of non-compliance by a Union institution or body with one of the measures referred to in points (d) to (h) and (j) of this paragraph, depending on the circumstances of each individual case;
  - p. to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisations.
  - q. The European Data Protection Supervisor shall have the following authorisation and advisory powers:
    - r. to advise data subjects in the exercise of their rights;
    - s. to advise the controller in accordance with the prior consultation procedure referred to in Article 40, and in accordance with Article 41(2);
    - t. to issue, on his or her own initiative or on request, Opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data;
    - u. to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 48(2);
    - v. to authorise contractual clauses referred to in point (a) of Article 48(3);
    - w. to authorise administrative arrangements referred to in point (b) of Article 48(3);
    - x. to authorise processing operations pursuant to implementing acts adopted under Article 40(4).
2. The European Data Protection Supervisor shall have the power to refer the matter to the Court of Justice under the conditions provided for in the Treaties and to intervene in actions brought before the Court of Justice..

3. The exercise of the powers conferred on the European Data Protection Supervisor pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedies and due process, set out in Union law.



The background of the page is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting numerous small, semi-transparent blue dots. These dots and lines are scattered across the entire page, creating a sense of digital connectivity and data flow. The lines vary in length and orientation, forming a web-like structure that is denser in some areas and sparser in others.

## **ANNEX C**

# **List of Data Protection Officers**

Council of the European Union	Reyes OTERO ZAPATA (DPO)
European Parliament	Secondo SABBIONI (DPO)
European Commission	Martin KRÖGER (DPO) Niels Bertil RASMUSSEN (Deputy DPO)
Court of Justice of the European Union	Joris PLINGERS (DPO) Ivana BOŽAC (Deputy DPO)
Court of Auditors	Elena MAPELLE (DPO)
European Economic and Social Committee (EESC)	Michele ANTONINI (DPO) Simone BAPTISTA (Deputy DPO)
Committee of the Regions (CoR)	Antonio FIGUEIRA (DPO) Jean-Sébastien IESARI-MARRE (Deputy DPO)
European Investment Bank (EIB)	Pelopidas DONOS (DPO) Laurence WAERENBURGH (Deputy DPO)
European External Action Service (EEAS)	Emese SAVOIA-KELETI (DPO)
European Ombudsman	Francesca PAVESI (DPO) Nicholas HERNANZ (Deputy DPO)

European Data Protection Board (EDPB)	<p>Joao SILVA (DPO)</p> <p>Nerea PERIS BRINES (Deputy DPO)</p> <p>Panagiota KALYVA (Deputy DPO)</p>
European Data Protection Supervisor (EDPS)	<p>Constantin CHIRA PASCANUT (DPO)</p> <p>Marco MORESCHINI (Deputy DPO)</p>
European Central Bank (ECB)	<p>Maarten DAMAN (DPO)</p>
European Anti-Fraud Office (OLAF)	<p>Veselina TZANKOVA (DPO)</p> <p>Christina KARAKOSTA (Deputy DPO)</p>
Translation Centre for the Bodies of the European Union (CdT)	<p>Martin GARNIER (DPO)</p>
European Union Intellectual Property Office (EUIPO)	<p>Gloria FOLGUERA VENTURA (DPO)</p>
Agency for Fundamental Rights (FRA)	<p>Luisa LOPEZ ALVARO (DPO)</p> <p>Sara SIGHINOLFI (Deputy DPO)</p>
Agency for the Cooperation of Energy Regulators (ACER)	<p>Marina ZUBAC (DPO)</p> <p>Stefano VAONA (Deputy DPO)</p>
European Medicines Agency (EMA)	<p>Stefano MARINO (DPO)</p> <p>Orsolya EÖTVÖS (Assistant DPO)</p>
Community Plant Variety Office (CPVO)	<p>Gloria FOLGUERA VENTURA (DPO)</p>

European Training Foundation (ETF)	Tiziana CICCARONE (DPO) Laurens RIJKEN (Deputy DPO)
European Asylum Support Office (EASO)	Maria Angeliki STAMATOPOULOU (DPO)
European Network and Information Security Agency (ENISA)	Athena BOURKA (DPO)
European Foundation for the Improvement of Living and Working Conditions (Eurofound)	Mafalda AGUIAREESC (DPO)
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	Ignacio VÁZQUEZ MOLINÍ (DPO)
European Food Safety Authority (EFSA)	Claus REUNIS (DPO)
European Maritime Safety Agency (EMSA)	Radostina NEDEVA MAEGERLEIN (DPO) Iris DE OLIVEIRA (Deputy DPO)
European Centre for the Development of Vocational Training (CEDEFOP)	Jesús BUSTAMANTE (DPO)
Education, Audiovisual and Culture Executive Agency (EACEA)	Nicolas DURAND (DPO) Anber EVANS (Deputy DPO)
European Agency for Safety and Health at Work (EU-OSHA)	Jan Ole VOSS (DPO)
European Fisheries Control Agency (EFCA)	Stefano DONADELLO (DPO) Marta RAMILA HIDALGO (Deputy DPO)
European Union Satellite Centre (SATCEN)	Joana GONÇALVES (DPO) Maria CHATZIANGELIDOU (Assistant DPO)

European Institute for Gender Equality (EIGE)	Ieva VASILIUONE (DPO) Nicasio LOPEZ RODRIGUEZ (Deputy DPO)
European GNSS Agency (GSA)	Ezio VILLA (DPO) Tina KOSIR
European Union Agency for Railways (ERA)	Zografia PYLORIDOU (DPO)
European Health And Digital Executive Agency (HaDEA)	Yolanda AREVALO TORRES (DPO) Anthony BISCH (Deputy DPO)
European Centre for Disease Prevention and Control (ECDC)	Riccardo MALACALZA (DPO)
European Environment Agency (EEA)	Olivier CORNU (DPO) Helle MOLLER (Deputy DPO) Eleni BARLA(Deputy DPO)
European Investment Fund (EIF)	Paolo SINIBALDI (DPO)
European Border and Coast Guard Agency (Frontex)	Nayra PEREZ (DPO) Julia ANTONOVA (Associate DPO)
European Securities and Markets Authority (ESMA)	Sophie VUARLOT-DIGNAC (DPO)
European Aviation Safety Agency (EASA)	Carla RAMOS (DPO) Elena TELLADO VÁZQUEZ (Deputy DPO)



European Innovation Council And SME's Executive Agency (EISMEA)	Elke RIVIERE (DPO)
European Climate, Infrastructure And Environment Executive Agency (CINEA)	Caroline MAION (DPO)
European Banking Authority (EBA)	Jonathan OVERETT SOMNIER (DPO)
European Chemicals Agency (ECHA)	Bo BALDUYCK (DPO)
European Research Council Executive Agency (ERCEA)	Roberta MAGGIO (DPO)
Research Executive Agency (REA)	Maria Francisca BRUNET-COMPANY (DPO) Sergejs TROFIMOV (Deputy DPO)
European Systemic Risk Board (ESRB)	Maarten DAMAN (DPO)
Fusion for Energy	Walter SCHUSTER (DPO) Raymond MONK (Deputy DPO)
SESAR Joint Undertaking	Laura GOMEZ GUTIERREZ (DPO) Vicenza DA SILVA (Deputy DPO)
ECSEL	Anne SALAÜN (DPO)
Clean Sky Joint Undertaking	Bruno MASTANTUONO (DPO)
Innovative Medicines Initiative Joint Undertaking (IMI)	Sebastien PECHBERTY (DPO) Desmond BARRY (Deputy DPO)



Fuel Cells & Hydrogen Joint Undertaking	Georgiana BUZNOSU (DPO)
European Insurance and Occupations Pensions Authority (EIOPA)	Catherine COUCKE (DPO)
European Agency for Law Enforcement Training (CEPOL)	Olli KALHA (DPO)
European Institute of Innovation and Technology (EIT)	Nora TOSICS (DPO)
European Defence Agency (EDA)	Clarisse RIBEIRO (DPO) Christina ENGEßER (Deputy DPO)
Body of European Regulators for Electronic Communications (BEREC)	Marco DE SANTIS (DPO)
European Union Institute for Security Studies (EUISS)	Nikolaos CHATZIMICHALAKIS (DPO)
eu-LISA	Encarna GIMENEZ (DPO)
Bio-Based Industries Joint Undertaking	Marta CAMPOS-ITURRALDE (DPO)
EUROPOL	Daniel DREWER (DPO)
EFTA Surveillance Authority (ESA)	Kjersti SNEVE (DPO)
Shift2Rail Joint Undertaking	Isaac GONZALEZ GARCIA (DPO)
Single Resolution Board (SRB)	Esther BRISBOIS (DPO)

EUROJUST	Diana ALONSO BLAS (DPO)
Authority For European Political Parties And European Political Foundations (APPF)	Secondo SABBIONI (DPO)
Bio-Based Industries Joint Undertaking (BBI JU)	Marta CAMPOS ITURRALDE (DPO)
European Labour Authority (ELA)	Jacek SALDAN
European Public Prosecutor's Office (EPPO)	Steven RYDER (DPO)
European High-Performance Computing Joint Undertaking (EuroHPC JU)	Lake THORSTEN (DPO)



## **ANNEX D**

# **List of EDPS Opinions**

Please refer to the [EDPS website](#) for translations and executive summaries.

In 2021, the EDPS issued Opinions on the following subjects (date of issuance in bold):

- [Opinion on the Digital Services Act \(DSA\)](#) **10/02/2021**
- [Opinion on the Digital Markets Act \(DMA\)](#) **10/02/2021**
- [Opinion on the conclusion of the EU and UK trade agreement and the EU & UK exchange of classified information agreement](#) **22/02/2021**
- [Opinion on the EUROPOL reform](#) **08/03/2021**
- [Opinion on Cybersecurity](#) **11/03/2021**
- [Opinion on Ledger technology](#) **23/04/2021**
- [Opinion on digital operational resilience for the financial sector \(DORA\)](#) **10/05/2021**
- [Opinion on the opening of negotiations for a cooperation agreement between EU and INTERPOL](#) **25/05/2021**
- [Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive \(EU\) 2019/1937 \(MICA\)](#) **25/06/2021**
- [Proposal for a Council Regulation on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing Regulation \(EU\) No 1053/2013](#) **27/07/2021**
- [Proposal for a Directive on consumer credits](#) **26/08/2021**
- [AML Package](#) **21/09/2021**




## **ANNEX E**

# **List of EDPS Formal Comments**

Please refer to the [EDPS website](#) for translations and executive summaries.

In 2021, the EDPS issued Formal Comments on the following subjects (date of issuance in bold):

- Implementing Decision use of ADIS and EUROPHYT, the issuance of electronic animal health certificates, official certificates, animal health/ official certificates and commercial documents, the use of electronic signatures, and the functioning of TRACES **14/01/2021**
- Draft Commission Implementing Regulation on the monitoring and reporting of data relating to CO2 emissions from passenger cars and light commercial vehicles pursuant to Regulation (EU) 2019/631 of the European Parliament and of the Council and repealing Implementing Regulations (EU) No 1014/2010, (EU) No 293/2012, (EU) 2017/1152 and (EU) 2017/1153 **14/01/2021**
- Commission Implementing Decision on the mechanism, the procedures and the appropriate requirements for data quality compliance, pursuant to Article 74(5) of Regulation (EU) 2018/1240 (ETIAS) **15/01/2021**
- Commission Implementing Decision laying down the content of the logs of automated scanned searches of the number plates of motor vehicles using Automatic Number Plate Recognition systems in the Schengen Information System (SIS) **21/01/2021**
- Commission Implementing Decision laying down the specifications and conditions for the EES website (EES) **21/01/2021**
- Implementing Decision on the detailed rules for the EES on the information to be provided to the European Commission by MS regarding the stamping of travel documents **21/01/2021**
- Proposal on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726 **26/01/2021**
- Commission Implementing Decision on measures or accessing, amending, erasing and advance erasing of data in the ETIAS Central System (ETIAS) **11/02/2021**
- Commission Implementing Decision defining the technical specification of the ETIAS watchlist and of the assessment tool (ETIAS) **15/02/2021**
- Consultation on the IA establishing the forms and the technical rules for the effective exchange of information via the Customs Information



system (CIS) provided for in Regulation (EU) No 2018/1672  
**12/02/2021**

- Proposal for a Council Regulation amending Council Regulation (EU) No 389/2012 on administrative cooperation in the field of excise duty  
**17/02/2021**
- Implementing Decision on the specifications for technical solutions to connect central access points to the ETIAS Central System  
**26/02/2021**
- COM(2020) 727 Proposal for a Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision **02/03/2021**
- COM(2020) 725 Proposal for a Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices **04/03/2021**
- COM(2020) 726 Proposal for establishing a European Centre for disease prevention **10/03/2021**
- Proposal for a Directive amending Council Framework Decision 2002/465/JHA, as regards its alignment with EU rules on the protection of personal data **10/03/2021**
- Proposal for a Directive on amending Directive 2014/41/EU, as regards its alignment with EU rules on the protection of personal data **10/03/2021**
- Implementing Reg. laying down rules for application of Dir.as regards technical specification and procedures for BRIS and repealing IR 2020/2244 **10/03/2021**
- Proposal for amendment of Regulation (EU) 2018/1862 on the use of SIS within the field of police and judicial cooperation as regards entry of alerts by Europol **10/03/2021**
- Draft Implementing Decisions laying down a standard form for notification of a RED LINK (design & development of interoperability)  
**31/03/2021**
- Consultation on Delegated Regulations laying down rules on the operation of the WEB PORTAL for the design and development of interoperability **31/03/2021**
- Draft Implementing Decision laying down the performance



requirements & practical arrangements for monitoring the performance of the shared Biometric Matching Service **31/03/2021**

- Proposal for a Decision on the position to be taken as regards the date on which provisional application of the EU-UK Trade and Cooperation Agreement shall cease **31/03/2021**
- Proposal for a regulation establishing the Brexit Adjustment Reserve (COM(2020) 854) **12/04/2021**
- Commission Implementing Regulation for the purposes of European Parliament and Council Regulation (EU) 2019/880 on the introduction and the import of cultural goods **22/04/2021**
- Draft Implementing decision laying down a standard form for notification of a WHITE LINK (design & development of interoperability) **22/04/2021**
- Proposal for a Reg. amending ECRIS-TCN on establishing a framework for interoperability between EU info systems for the purpose of introducing a screening of 3rd country nationals at the external borders **27/04/2021**
- ETIAS delegated regulations on the payment methods and collection process for the travel authorisation fee **27/04/2021**
- Delegated regulation with regard to cases where identity data may be considered as same or similar for the purpose of the multiple identity detection **27/04/2021**
- Proposal for a Directive of the European Parliament and of the Council to strengthen the application of the principle of equal pay for equal work or work of equal value between men and woman **27/04/2021**
- Implementing Reg. laying down rules & conditions for the operation of the web service and data protection and security rules applicable to the web service **29/04/2021**
- Implementing Reg. laying down the rules and conditions for verification queries by carriers, provisions for data protection and security for the carriers' authentication scheme as well as fall back procedures in case of technical impossibility **30/04/2021**
- Implementing Reg. laying down the details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data **30/04/2021**

- Implementing Decisions laying down the specifications of the cooperation procedure in the event of a security incident **06/05/2021**
- Implementing Act on alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through PLF **06/05/2021**
- Implementing Act setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the “once-only” principal **06/05/2021**
- Implementing Decision on the requirements for the means of AUDIO & VIDEO communication for the interview (ETIAS) **10/05/2021**
- Commission Implementing Decisions laying down the technical details of the profiles for the users of the European search portal (ESP profiles) **17/05/2021**
- Implementing Decisions specifying the technical procedure for the European search portal to query the EU information systems, Europol data and Interpol databases and the format of the European search portal’s replies **17/05/2021**
- Implementing Decisions laying down the technical rules for creating links between data from different EU information systems **17/05/2021**
- Regulatory Technical Standard (RTS) containing a template document for cooperation arrangements with 3rd countries **25/05/2021**
- Implementing Decision laying down STANDARD FORM for refusal, annulment or revocation of a travel authorisation **25/05/2021**
- 2 Implementing Decisions: 1. SIRENE Manual-Borders and return 2. SIRENE Manual-Police **02/06/2021**
- Implementing Decision on specifying the RISKS as defined in Regulation (EU) 2018/1240 as well as in the Commission Delegated Decision **02/06/2021**
- Implementing Decision laying down a model security plan, a model business continuity and a disaster recovery plan pursuant to Article 59(4) of Regulation (EU) 2018/1240 **07/06/2021**
- Commission Delegated Decision on further defining the risks related to security or illegal immigration or high epidemic risk **07/06/2021**
- Commission implementing regulation laying down implementing

technical standards for the application of Regulation (EU) No 596/2014 of the European Parliament and of the Council with regard to the format of insider lists and their updates **07/06/2021**

- Proposal for Regulation on laying down conservation and management measures applicable in the Western and Central Pacific Fisheries Convention Area COM(2021)198 **14/06/2021**
- Implementing regulation amending implementing regulation (EU) 79/2012 on automated access to the information on the VAT exempted importations under the 'import scheme' **17/06/2021**
- Implementing Decision on detailed rules on the operation of the central repository for reporting and statistics **17/06/2021**
- Commission Delegated Decision specifying the content and format of the predetermined list of options to be used for the purpose of requesting additional info or documentation **21/06/2021**
- Proposal for an Implementing decision laying down technical specifications & rules for the implementation of the trust framework for the EU DCC **22/06/2021**
- Proposal for a Regulation of the European Parliament and of the Council on foreign subsidies distorting the internal market **29/06/2021**
- Recommendation for a Council Decision authorising negotiations for an EU-UK Competition Cooperation Agreement **05/07/2021**
- Legislative consultation on a draft Commission Implementing Regulation on the functionalities of the public interface connected to the Internal Market Information System for posting drivers in road transport **06/07/2021**
- Draft Commission Implementing Regulation on the European Database on Medical Devices (Eudamed) **09/07/2021**
- Proposal for an implementing decision on alerts triggered by serious cross-border threats to health in the context of the Passenger Locator Form (PLF) **13/07/2021**
- Recommendation for a Council decision authorising the opening of negotiations to amend the Agreement between the European Union and Japan on mutual legal assistance in criminal matters and its Annex **16/07/2021**
- Proposals for decisions on the conclusion and on the signing of the Implementing Protocol (2021-2026) to the Fisheries Partnership

Agreement between the Gabonese Republic and the EC **19/07/2021**

- Proposal for a Regulation of amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity **27/07/2021**
- Proposal for a Regulation for a Directive on the resilience of critical entities **11/08/2021**
- Proposal for a regulation on general product safety **18/08/2021**
- Proposal for a Council Decision on the accession of the European Union to the Convention on the Conservation and Management of High Seas Fisheries Resources in the North Pacific Ocean **27/08/2021**
- Implementing Regulation laying down detailed rules for the application of Council Regulation (EU) No 904/2010, as regards the special scheme for small enterprises **24/09/2021**
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2019/1153 of the European Parliament and of the Council, as regards access of competent authorities to centralised bank account registries through the single access point **06/09/2021**
- Implementing Decision on Risk pursuant to Reg. (EU) 2018/1672 (The Cash Controls Regulation) **14/09/2021**
- Proposal for a Regulation laying down conservation & management measures for the conservation of the Southern Bluefin Tuna **20/09/2021**
- Commission Implementing Decisions for technical solutions to manage user access requests and information collection for Regulation (EU) 2019/817 and (EU) 2019/817 **28/09/2021**
- Proposals for a COUNCIL DECISION on SFPA between the EU and Mauritania + implementing protocol **14/10/2021**
- Implementing Decision amending Implementing Decision (EU) 2021/1073 laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate **18/10/2021**
- Consultation on the draft Commission Implementing Regulation on the electronic interface and data exchange between national customs systems and the EU Information and Communication System for Market Surveillance (ICSMS) **22/10/2021**

- Proposal for a decision on the signing and provisional application of the Protocol (2021-2024) on the implementation of the Sustainable Fisheries Partnership Agreement between the European Union and the Cook Islands **03/11/2021**
- Draft Commission Delegated Regulations supplementing Directive 2010/40/EU of the European Parliament and the Council with regard to the provision of EU-wide real-time traffic information services (PLAN/2020/7494) **08/12/2021**
- Laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate and on the Annex as regards the validity of vaccination certificates issued under the EU Digital COVID Certificate framework **14/12/2021**
- Establishment of a system of digital Passenger Locator Forms (PLF) as part of the procedures for the notification of alerts within the early warning and response system established in relation to serious cross-border threats to health **14/12/2021**
- Implementing regulation on paying agencies and other bodies, financial management, clearance of accounts, rules on checks, securities and transparency **09/12/2021**



## **ANNEX F**

# **List of EDPS-EDPB Joint Opinions**

In 2021, the EDPS-EDPB issued Joint Opinions on the following subjects (date of issuance in bold):


- Joint opinion on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries **18/01/2021**
- Joint Opinion 1/2021 on the European Commission's Implementing Decision on standard contractual clauses between controllers and processors **18/01/2021**
- Joint Opinion on EU Regulation on European Data Governance (Data Governance Act) **08/03/2021**
- Joint Opinion on Digital Green Pass **31/03/2021**
- Joint Opinion on the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) **16/06/2021**

The background of the slide features a dark blue gradient with a complex, abstract network of thin, light blue lines and dots. These lines and dots are interconnected, forming a web-like structure that covers the entire page. The dots vary in size and brightness, with some appearing as small, faint points and others as larger, more prominent nodes. The lines are thin and light blue, creating a subtle but intricate pattern.

## **ANNEX G**

# **EDPS work within the EDPB**





Number of files for which the EDPS made a substantial contribution to -  
in particular as lead rapporteur, rapporteur or member of a drafting team  
- in the context of the EDPB for the year 2021:

- EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors;
- EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries;
- Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive;
- EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research;
- Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention);
- EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act);
- Statement 03/2021 on the ePrivacy Regulation;
- EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery;
- Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom;
- Guidelines 03/2021 on the application of Article 65(1)(a) GDPR;
- Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom;
- Statement 05/2021 on the Data Governance Act in light of the legislative developments;
- EDPB Response to Mr. de Serpa Soares, Under-Secretary-General for Legal Affairs and UN Legal Counsel (May 2021);

- EDPB response to Mr Miguel de Serpa Soares regarding the ongoing dialogue between the EDPB and the United Nations on data protection (November 2021);
- Final version of the Recommendations 1/2020 on supplementary measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (after public consultation);
- EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act);
- Opinion 20/2021 on Tobacco Traceability System;
- EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro - to the European Central Bank;
- Guidelines 02/2021 on virtual voice assistants (after public consultation);
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR (after public consultation);
- Guidelines 10/2020 on restrictions under Article 23 GDPR;
- EDPS proposal on 2022 coordinated action of the EDPB in the context of the Coordinated Enforcement Framework;
- Statement on the Digital Services Package and Data Strategy;
- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR;
- Guidelines 01/2021 on Examples regarding Personal Data Breach Notification;
- Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject;
- Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62;

- Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea;
- Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited;
- Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR.

The background of the entire page is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting various-sized dots. Some dots are larger and more prominent, while others are smaller and less distinct. The lines and dots are scattered across the page, creating a sense of interconnectedness and depth.

## **ANNEX H**

# **The Supervisor's Speeches**

## European Parliament

Wojciech Wiewiórowski, speech at the 8th Joint Parliamentary Scrutiny Group on Europol, Brussels (1 February 2021) via video link.

Wojciech Wiewiórowski , hearing on the Data Governance Act - Speech before Committee on Civil Liberties, Justice and Home Affairs (LIBE) in hearing on the Data Governance Act, Brussels (16 March 2021).

Wojciech Wiewiórowski, presentation of the EDPB-EDPS Joint Opinion on the Digital Green Certificate to the Committee on Civil Liberties, Justice and Home Affairs (LIBE), Brussels (13 April 2021).

Wojciech Wiewiórowski, presentation of the EDPS Annual Report 2020 by Wojciech Wiewiórowski to the Committee on Civil Liberties, Justice and Home Affairs (LIBE), Brussels (19 April 2021).

Wojciech Wiewiórowski, remarks by the European Data Protection Supervisor Wiewiórowski, at the Committee on Civil Liberties, Justice and Home Affairs (LIBE) meeting on the follow-up to the EDPS admonishment of Europol, Brussels (16 June 2021).

Wojciech Wiewiórowski, speech at the 9th meeting of the Europol Joint Parliamentary Scrutiny group, Brussels (25 October 2021).

Wojciech Wiewiórowski, LIBE Committee exchange of views on Pegasus spyware (29 November 2021).

## Council

Wojciech Wiewiórowski, Informal videoconference of the members of the Working Party on Data Protection, Brussels (22 January 2021) via video link.

## International Conferences

Wojciech Wiewiórowski, speech at the EDPS- Civil Society Summit, Privacy Camp 2021, Brussels(26 January 2021) via video link.

Wojciech Wiewiórowski, "Data Privacy Day: A Global Vision for Maintaining Trust", World Bank group, virtual event (28 January 2021) via video link.

Wojciech Wiewiórowski Keynote online international conference Digital transformation and data protection in a pandemic world, EU project ARC (28 January 2021) via video link.

Wojciech Wiewiórowski Croatian Employers Association and IAPP KnowledgeNet Chapter Croatia - Data Privacy Day online conference (28 January 2021) via video link.

Wojciech Wiewiórowski, CPDP: Data Protection and Artificial Intelligence, (Brussels, 29 January 2021) via video link.

Wojciech Wiewiórowski, Speaker: Mentor Group Webcast Series – Forum for EU-US Legal-Economic Affairs, Brussels (30 March 2021) via video link.

Wojciech Wiewiórowski, 3rd Virtual EDPS-DPO Meeting Brussels (4 June 2021) via video link.

Wojciech Wiewiórowski, Internet Privacy Engineering Network (IPEN) webinar: "Synthetic data: what use cases as a privacy enhancing technology?", Brussels (16 June 2021) via video link.

Wojciech Wiewiórowski, Annual Privacy Forum 2021, Warsaw (17 June 2021) via video link.

Wojciech Wiewiórowski, International Conference and launch of the South EU Google Data Governance Chair, Madrid (24 June 2021) via video link.

Wojciech Wiewiórowski, 7th EDEN Event on Data Protection in Law event, "Human After All: Data Protection in Policing", Rome (18 October 2021) via video link.

## Other events

Wojciech Wiewiórowski, Privacy law salon, Brussels (24 February 2021) via video link.

Wojciech Wiewiórowski, Guest lecture at University of Warsaw, Brussels (11 March 2021) via video link.

Wojciech Wiewiórowski, Clusit Security Summit 2021, Milan (18 March 2021) via video link.

Wojciech Wiewiórowski, 4th National Data Privacy Awareness Week Conference (PAW 2021) (27 May 2021) via video link.

Wojciech Wiewiórowski, speaker at Turkish Industry and Business Association, Personal Data Protection Conference, Ankara (8 June 2021) via video link.

Wojciech Wiewiórowski, ERA Online Annual Conference on European Data Protection Law 2021, Brussels (9 June 2021) via video link.

Wojciech Wiewiórowski, keynote speech at the EPPA Symposium (College of Europe), Brugge (15 June 2021) via video link.

Wojciech Wiewiórowski, Regulatory challenges and opportunities in data protection - an EDPS perspective, ISMS Forum, Madrid (3 December 2021).

The background of the slide is a dark blue gradient. Overlaid on this is a complex, abstract network of thin, light blue lines connecting numerous small, semi-transparent blue dots. These dots and lines are scattered across the entire frame, creating a sense of global connectivity and digital infrastructure. The text is centered in the middle of the image.

# **GETTING IN TOUCH WITH THE EU**



## In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

## On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696 or
- by email via: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

## Finding information about the EU

### Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: [https://europa.eu/european-union/index\\_en](https://europa.eu/european-union/index_en)

## EU publications

You can download or order free and priced EU publications at: <https://publications.europa.eu/en/publications>

Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)).

## EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: <http://eur-lex.europa.eu>

## Open data from the EU

The EU Open Data Portal (<http://data.europa.eu/euodp/en>) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.



Twitter:

@EU\_EDPS



LinkedIn:

EDPS



YouTube:

European Data Protection Supervisor



Publications Office  
of the European Union



EDPS